TOSHIBA
Wireless Routing Center
WRC-1000
User's Manual

R10UM020801

Copyright

© 2001-2002 by TOSHIBA Corporation. All rights reserved. Under the copyright laws, this manual cannot be reproduced in any form without the prior written permission of TOSHIBA. No patent liability is assumed, with respect to the use of the information contained herein.

TOSHIBA Wireless Routing Center WRC-1000 User's Manual

First edition August 2002

Disclaimer

This manual has been validated and reviewed for accuracy. The instructions and descriptions it contains are accurate for the *TOSHIBA Wireless Routing Center WRC-1000 User's Manual* at the time of this manual's production. However, succeeding devices and manuals are subject to change without notice. TOSHIBA assumes no liability for damages incurred directly or indirectly from errors, omissions or discrepancies between the device and the manual.

Trademarks

Microsoft, Windows, NetMeeting and Windows® Messenger are registered trademarks of Microsoft Corporation.

Ethernet is a registered trademark of Xerox Corporation.

Wi Fi CERTIFIED™ is a Certification Mark of the Wireless Ethernet Compatibility Alliance, Inc.

Adobe and Adobe Acrobat are registered trademarks of Adobe Systems Incorporated.

Other trademarks and registered trademarks not listed above may be used in this manual.

FCC information

Product Name : **TOSHIBA Wireless Routing Center WRC-1000**

Model number : **PA3227**

FCC notice "Declaration of Conformity Information"

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

> ***WARNING:*** *TOSHIBA is not responsible for any radio or television interference caused by unauthorized modification of the devices included with this TOSHIBA Wireless Routing Center, or the substitution or attachment of connecting cables and equipment other than specified by TOSHIBA. The correction of interference caused by such unauthorized modification, substitution or attachment will be the responsibility of the user.*

FCC conditions

This device complies with part 15 of the FCC Rules. Operation is subject to the Following two conditions:

1. This device may not cause harmful interference.
2. This device must accept any interference received, including interference that may cause undesired operation.

Contact

Address: TOSHIBA America Information Systems, Inc.
9740 Irvine Boulevard
Irvine, California 92618-1697

Telephone: (949) 583-3000

EU Declaration of Conformity

TOSHIBA declares, that the product: PA3227U/PA3227E/PA3227A/ PAWRC001 conforms to the following Standards:

Supplementary Information: "The product complies with the requirements of the Low Voltage Directive 73/23/EEC and the EMC Directive 89/336/EEC."

This product is carrying the CE-Mark in accordance with the related European Directives. Responsible for CE-Marking is TOSHIBA Europe, Hammfelddamm 8, 41460 Neuss, Germany.

VCCI Class B Information

この装置は、情報処理装置等電波障害自主規制協議会（ＶＣＣＩ）の基準に基づくクラスＢ情報技術装置です。この装置は、家庭環境で使用することを目的としていますが、この装置がラジオやテレビジョン受信機に近接して使用されると、受信障害を引き起こすことがあります。
取扱説明書に従って正しい取り扱いをして下さい。

Wireless LAN information

Wireless Interoperability

The TOSHIBA Wireless Routing Center WRC-1000 products are designed to be interoperable with any Wireless LAN product that is based on Direct Sequence Spread Spectrum (DSSS) radio technology, and is compliant to:

- The IEEE 802.11 Standard on Wireless LANs (Revision B), as defined and approved by the Institute of Electrical and Electronics Engineers.
- The Wireless Fidelity (WiFi) certification as defined by the WECA Wireless Ethernet Compatibility Alliance.

Wireless LAN and your Health

Wireless LAN products, like other radio devices, emit radio frequency electromagnetic energy. The level of energy emitted by Wireless LAN devices however is far much less than the electromagnetic energy emitted by wireless devices like for example mobile phones.

Because Wireless LAN products operate within the guidelines found in radio frequency safety standards and recommendations, TOSHIBA believes Wireless LAN is safe for use by consumers. These standards and recommendations reflect the consensus of the scientific community and result from deliberations of panels and committees of scientists who continually review and interpret the extensive research literature.

In some situations or environments, the use of Wireless LAN may be restricted by the proprietor of the building or responsible representatives of the organization. These situations may for example include:

- Using the Wireless LAN equipment on board of aeroplanes, or
- In any other environment where the risk of interference to other devices or services is perceived or identified as harmful.

If you are uncertain of the policy that applies on the use of wireless devices in a specific organization or environment (e.g. airports), you are encouraged to ask for authorization to use the Wireless LAN device prior to turning on the equipment.

Regulatory Information

The *TOSHIBA Wireless Routing Center WRC-1000* must be installed and used in strict accordance with the manufacturer's instructions as described in the user documentation that comes with the product. This device complies with the following radio frequency and safety standards.

Canada - Industry Canada (IC)

This device complies with RSS 210 of Industry Canada.

Operation is subject to the following two conditions: (1) this device may not cause interference, and (2) this device must accept any interference, including interference that may cause undesired operation of this device."

L'utilisation de ce dispositif est autorisée seulement aux conditions suivantes : (1) il ne doit pas produire de brouillage et (2) l' utilisateur du dispositif doit étre prét à accepter tout brouillage radioélectrique reçu, même si ce brouillage est susceptible de compromettre le fonctionnement du dispositif.

The term "IC" before the equipment certification number only signifies that the Industry Canada technical specifications were met.

Approval Number: 1353A-WLL030

To prevent radio interference to the licensed service, this device is intended to be operated indoors and away from windows to provide maximum shielding. Equipment (or its transmit antenna) that is installed outdoors is subject to licensing.

Pour empecher que cet appareil cause du brouillage au service faisant l'object d'une licence, il doit Etre utilise a l'interieur et devrait etre place loin des fenetres afin de fournir un ecran de blindage Maximal. Si le materiel (ou son antenne d'emission) est installe a l'exterieur, il doit faire l'objet D'une license.

Europe - EU Declaration of Conformity

This device complies with the essential requirements of the R&TTE Directive 1999/5/EC with essential test suites as per standards:

- EN 60950 Safety of Information Technology equipment
- ETS 300 328 Technical requirements for radio equipment
- ETS 300 826 General EMC requirements for radio equipment.

België/ Belgique:

For outdoor usage only channel 10 (2457 MHz) and 11 (2462 MHz) is allowed.

For private usage outside buildings across public grounds over less than 300m no special registration with IBPT/BIPT is required. Registration to IBPT/BIPT is required for private usage outside buildings across public grounds over more than 300m. An IBPT/BIPT license is required for public usage outside building.

For registration and license please contact IBPT/BIPT.

Gebruik buiten gebouw alleen op kanalen 10 (2457 MHz) en 11 (2462 MHz). Voor privé-gebruik buiten gebouw over publieke groud over afstand kleiner dan 300m geen registratie bij BIPT/IBPT nodig; voor gebruik over afstand groter dan 300m is wel registratie bij BIPT/IBPT nodig. Voor publiek gebruik buiten gebouwen is licentie van BIPT/IBPT verplicht. Voor registratie of licentie kunt u contact opnemen met BIPT.

L'utilisation en extérieur est autorisé sur le canal 10 (2457 MHz) et 11 (2462 Mhz).

Dans le cas d'une utilisation privée, à l'extérieur d'un bâtiment, au-dessus d'un espace public, aucun enregistrement n'est nécessaire pour une distance de moins de 300m. Pour une distance supérieure à 300m un enregistrement auprès de I'IBPT est requise. Pour une utilisation publique à I'extérieur de bâtiments, une licence de I'IBPT est requise. Pour les enregistrements et licences, veuillez contacter I'IBPT.

Deutschland:

License required for outdoor installations. Check with reseller for procedure to follow.

Anmeldung im Outdoor-Bereich notwendig, aber nicht genehmigungspflichtig. Bitte mit Händler die Vorgehensweise abstimmen.

France:

Restricted frequency band: only channels 10 and 11 (2457 MHz and 2462 MHz respectively) may be used in France. License required for every installation, indoor and outdoor installations. Please contact ART for procedure to follow.

Bande de fréquence restreinte : seuls les canaux 10 à 11 (2457 et 2462 MHz respectivement) doivent être utilisés en France.

Toute utilisation, qu'elle soit intérieure ou extérieure, est soumise à autorisation. Vous pouvez contacter I'Autorité de Régulation des Télécommuniations (http://www.art-telecom.fr) pour la procédure à suivre.

Italia:

License required for indoor use. Use with outdoor installations not allowed

E'necessaria la concessione ministeriale anche per l'uso interno.

Verificare con i rivenditori la procedura da seguire. L'uso per installazione in esterni non e' permessa.

Nederland:

License required for outdoor installations. Check with reseller for procedure to follow

Licentie verplicht voor gebruik met buitenantennes. Neem contact op met verkoper voor juiste procedure

USA-Federal Communications Commission (FCC)

This device complies with Part 15 of FCC Rules. Operation of the devices in a Wireless LAN System is subject to the following two conditions:

- This device may not cause harmful interference.
- This device must accept any interference that may cause undesired operation.

TOSHIBA is not responsible for any radio or television interference caused by unauthorized modification of the *TOSHIBA Wireless Routing Center WRC-1000*, or the substitution or attachment of connecting cables and equipment other than specified by TOSHIBA.

The correction of interference caused by such unauthorized modification, substitution or attachment will be the responsibility of the user.

> ***CAUTION:*** *Exposure to Radio Frequency Radiation.*

The radiated output power of the *TOSHIBA Wireless Routing Center WRC-1000* is far below the FCC radio frequency exposure limits. Nevertheless, the *TOSHIBA Wireless Routing Center WRC-1000* shall be used in such a manner that the potential for human contact during normal operation is minimized. When using this device, a certain separation distance between antenna and nearby persons has to be kept to ensure RF exposure compliance. The distance between the antennas and the user should not less than 20cm. Refer to the Regulatory Statements as identified in the documentation that comes with those products for additional information.

Using this equipment in Japan

In Japan, the frequency bandwidth of 2,400~2,483.5MHz for second generation low-power data communication systems such as this equipment overlaps that of mobile object identification systems (premises radio station and specified low-power radio station).

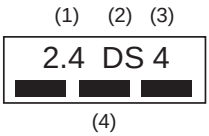
1. Sticker

   Please put the following sticker on devices incorporating this product.

> In the frequency bandwidth of this equipment, industrial device, scientific device, medical device like microwave oven, licensed premises radio station and non-licensed specified low-power radio station for mobile object identification system (RF-ID) that is used in product line of factories, (Other Radio Stations) are used.
>
> 1 Please make sure before using this equipment that no Other Radio Stations are used in the neighborhood.
>
> 2 In case that RF interference occurs to Other Radio Stations from this equipment, please change promptly the frequency for use, place to use, or stop emitting Radio.
>
> 3 Please contact TOSHIBA Direct PC if you have a problem, such as interference from this equipment to Other Radio Stations.

2. Indication

   The indication shown below appears on this equipment.



   (1) 2.4 : This equipment uses a frequency of 2.4 GHz.

   (2) DS : This equipment uses DS-SS modulation.

   (3) 4 : The interference range of this equipment is less than 40 m.

   (4) ▬ ▬ ▬ : This equipment uses a frequency bandwidth from 2,400 MHz to 2,483.5 MHz. It is possible to avoid the band of mobile object identification systems.

3. TOSHIBA Direct PC

Monday — Friday	: 10:00 — 17:00
Toll Free Tel	: 0120-13-1100
Direct Dial	: 03-3457-5916
FAX	: 03-5444-9450

Device Authorization

This device obtains the Technical Regulation Conformity Certification and the Technical Conditions Compliance Approval, and it belongs to the device class of radio equipment of low-power data communication system radio station stipulated in the Radio Law and the Telecommunications Business Law of Japan.

The Name of the radio equipment : WLL032

TELECOM ENGINEERING CENTER

Approval Number: 01NYDA1271, 01GZA1144

The following restrictions apply:

- Do not disassemble or modify the device.
- Do not install the embedded wireless module into other device.

Approved Countries/regions for use

This equipment is approved to the radio standard by the countries/regions listed in the table below.

CAUTION: *Do not use this equipment except in the countries/regions in the following table.*

Australia	Austria	Belgium
Canada	Denmark	Finland
France	Germany	Greece
Iceland	Ireland	Italy
Japan	Lichtenstein	Luxembourg
The Netherlands	Norway	Portugal
Spain	Sweden	Switzerland
UK	USA	

Countries/regions that have been approved
TOSHIBA Wireless Routing Center WRC-1000

Table of Contents

Preface

Manual contents ..... **xv**
Conventions ..... **xv**
Abbreviations xv
Icons xvi
Keys xvi
Key operation xvi
Display xvi
Messages xvi

Chapter 1 Introduction

Overview **1-1**
Package contents **1-1**
System requirements **1-1**
Features **1-2**
WAN port features 1-2
LAN port features 1-2
Router features 1-2
Security features 1-3
Wireless LAN features 1-3
Configuration and Management features 1-3

Chapter 2 The Grand Tour

Front, left and top **2-1**
Bottom and right **2-2**
Back **2-2**
Indicators **2-3**
Front Panel 2-3
LED Indicators 2-4
Stand **2-5**
Screws for wall mount **2-5**
AC adapter and power cord **2-6**

Chapter 3 Setup

Mounting **3-2**
Vertical mounting 3-2
Horizontal mounting 3-3
Wall mounting 3-4
AC adapter **3-4**
Connecting the Wireless Routing Center **3-5**
Setting up the Ethernet/Wireless LAN client **3-7**
Setting up Ethernet client 3-7
Setting up Wireless client 3-11
Checking Connection with the Wireless Routing Center 3-12

Chapter 4 Web Configuration

Accessing Web Configuration Page **4-2**
To enable your settings **4-7**
Viewing system overview and log **4-7**
Overview Configuration 4-7
Filter Log 4-8
Configuration for NAT Routing Mode **4-9**
WAN Configuration for NAT Routing Mode 4-9
LAN Configuration for NAT Routing Mode 4-13
Configuration for Bridge Mode **4-16**
Wireless LAN Configuration **4-18**
Basic 4-18
Advanced 4-19
Wireless LAN Security **4-19**
802.1x 4-20
WEP 4-20
Access Control 4-22
RADIUS Server 4-22
Filters **4-23**
Specifying IP Filter Rules 4-23
Filter Types 4-24
Forwarding **4-26**
Setting Up Forwarding Entries 4-26
If you have a Web server on your network… 4-27
Routing **4-29**
Administration Configuration **4-30**
System Configuration **4-32**

Chapter 5 Troubleshooting

Power 5-1
Ethernet 5-1
Configuration window 5-1
Wireless LAN 5-3
Application problems 5-7
Forgotten password 5-8
Question 5-8

Appendixes

Appendix A
Default values A-1

Appendix B
802.1x B-1

Appendix C
AC Power Cord and Connectors C-1

Glossary

Index

Preface

Congratulations on your purchase of the TOSHIBA Wireless Routing Center WRC-1000. The WRC-1000 provides high-speed wireless or wired connection to the Internet and to a Local Area Network.

This manual tells how to set up and begin using your TOSHIBA Wireless Routing Center WRC-1000, herein referred to as the Wireless Routing Center.

Manual contents

This manual is composed of five chapters, three appendixes and an index.

Chapter 1, *Introduction*, is an overview of the device's features and capabilities.

Chapter 2, *The Grand Tour*, describes devices and components.

Chapter 3, *Setup*, tells how to connect and setup your LAN devices.

Chapter 4, *Web Configuration*, tells how to configure the Wireless Routing Center via Web browser.

Chapter 5, *Troubleshooting*, suggests courses of action if the device doesn't seem to be working properly.

Appendix A lists all default settings.

Appendix B describes the 802.1x function.

Appendix C describes the power cord and connectors.

The Index quickly directs you to the information contained in this manual.

Conventions

This manual uses the following formats to describe, identify, and highlight terms and operating procedures.

Abbreviations

On first appearance, and whenever necessary for clarity, abbreviations are enclosed in parentheses following their definition. For example: Read Only Memory (ROM). Acronyms are also defined in the Glossary.

Icons

Icons identify ports, dials, and other parts of your Wireless Routing Center. The indicator panel also uses icons to identify the components it is providing information on.

Keys

The keyboard keys are used in the text to describe many computer operations. A distinctive typeface identifies the key top symbols as they appear on the keyboard. For example, **Enter** identifies the Enter key.

Key operation

Some operations require you to simultaneously use two or more keys. We identify such operations by the key top symbols separated by a plus sign (+). For example, **Ctrl + C** means you must hold down **Ctrl** and at the same time press **C**. If three keys are used, hold down the first two and at the same time press the third.

ABC When procedures require an action such as clicking an icon or entering text, the icon's name or the text you are to type in is represented in the type face you see to the left.

Display

ABC Names of Windows® or icons or text generated by the computer that appears on its display screen is presented in the type face you see to the left.

Messages

Messages are used in this manual to bring important information to your attention. Each type of message is identified as shown below.

> ***CAUTION:*** *Pay attention! A caution informs you that improper use of equipment or failure to follow instructions may cause data loss or damage your equipment.*

> ***NOTE:*** *Please read. A note is a hint or advice that helps you make best use of your equipment.*

Chapter 1

Introduction

Overview

The Wireless Routing Center features a wireless Access Point, a four-port LAN switch and a WAN port, which extend your existing broadband Cable/ADSL connection. It allows the broadband connection to be shared through either the IEEE 802.11b Access Point feature or the 10/100Base-TX Ethernet® switch, which also eliminates the need for an additional hub or switch.

The integrated DHCP server automatically assigns IP addresses to your LAN devices, and with the built-in Network Address Translation (NAT) function, your LAN is protected against outside intruders. The router can also be configured to filter internal access to the Internet. It is designed to provide a reliable Internet access solution for the corporate environment, the small office and the home user.

Package contents

Refer to the Quick Start Guide for the Equipment checklist. If any of the items is missing, contact your dealer.

System requirements

- Broadband Internet connection using Cable/ADSL modem for Internet connection
- One computer with 10/100Base-T Ethernet card and TCP/IP protocol installed for initial setup
- Internet Explorer 5.0 or higher for Web configuration
- Requirement for each computer on the LAN:

  — TCP/IP protocol installed

Features

WAN port features

- One 10/100 Base-TX RJ-45 auto sensing and crossover Ethernet WAN port for Broadband connection (Cable/DSL or direct Ethernet)
- PPPoE (PPP over Ethernet) Client with Keep Alive/Connect On Demand Support
- PAP and CHAP Authentication
- DHCP Client
- MAC Address Cloning
- Settable and Changeable IP Address

LAN port features

- Four RJ-45 LAN ports for 10/100Base-TX auto sensing & crossover Ethernet Switch LAN connection
- DHCP Server
- IP Address setting and changing

Router features

- NAT
- Firewall Support
- Bridge Mode Support
- IP Filtering
- IP Forwarding
- Static Routing
- DMZ Hosting
- DNS Forwarding
- DNS Relay
- UPnP Support (Windows Messenger® for Windows XP)*

Security features

- ASCII/HEX Format 64/128 Bit WEP Key for Wireless LAN
- IEEE 802.1x for Wireless LAN
- Allow List for Wireless LAN
- Supports IP packets filtering based on MAC Address, IP address, port number and protocol
- VPN Support (IPSec Passthrough, and PPTP Passthrough)

Wireless LAN features

- Fully compatible to IEEE 802.11b standard
- Direct Sequence Spread Spectrum (DSSS) technology
- Seamless roaming within Wireless LAN infrastructure
- Low power consumption for wireless client via efficient power management

Configuration and Management features

- Configurable through Web Browser via WAN/LAN
- Software Upgradeable
- DHCP Server function for IP distribution to local network users
- NTP/Manual System Clock
- Configuration Saving/Retrieving
- Event Logging

* This device has been tested by TOSHIBA in accordance with UPnP Forum Test Tools and is verified to support UPnP for Windows Messenger® for Windows XP.

The Grand Tour

This chapter identifies the various components of your Wireless Routing Center.

Front, left and top

Figure 2-1 shows the Wireless Routing Center's front, left and top positions.

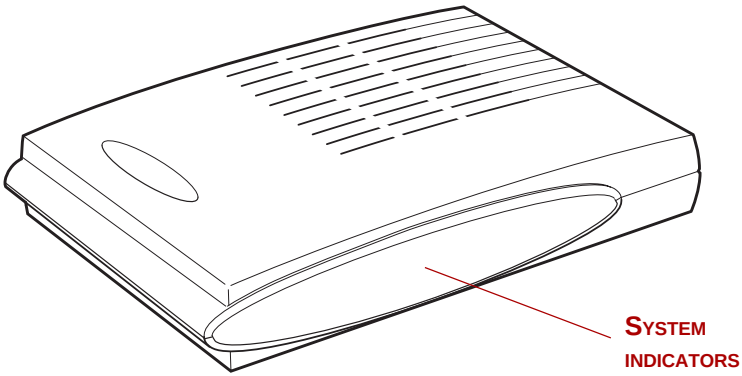


Figure 2-1 Front, left and top of the Wireless Routing Center

System indicators The system indicators provide LEDs for monitoring the Power, Wireless LAN LINK, Wireless LAN ACT, WAN, Ethernet 1, Ethernet 2, Ethernet 3 and Ethernet 4.

Bottom and right

Figure 2-2 shows the Wireless Routing Center's bottom and right sides.

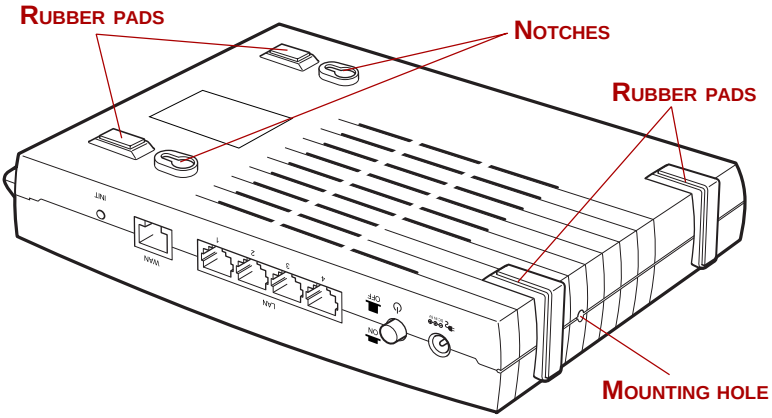


Figure 2-2 The bottom and right sides of the Wireless Routing Center

Notches Use these notches to hang the Wireless Routing Center from screws in a wall.

Rubber pads Use these pads to horizontal mount the Wireless Routing Center. Lay it on a flat surface with the pad side down.

Mounting hole Fit pin on the stand into mounting hole to use the Wireless Routing Center in an upright position.

Back

Figure 2-3 shows the Wireless Routing Center's back side.

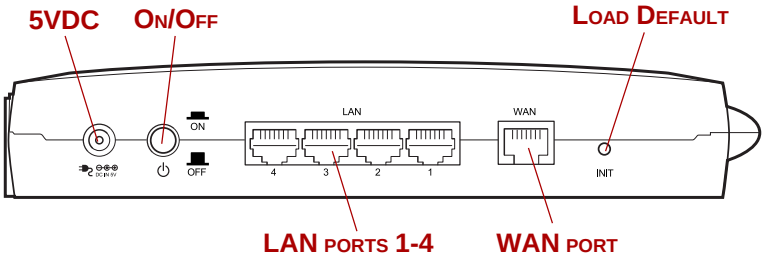
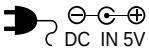


Figure 2-3 The back side of the Wireless Routing Center

5VDC Power connector



CAUTION: *Always use the correct AC adapter to avoid the risk of fire or damage to your Wireless Routing Center. The current rating for the Wireless Routing Center is 2.0 amperes.*

On/Off Power switch

LAN ports 1-4
LAN An integrated four-port 10/100BaseT switch provides four RJ-45 ports for connection to a hub, switch or NIC-equipped computer in your network. The LAN ports support Auto-MDIX feature which eliminates the need for crossover cables.

WAN port
WAN One RJ-45 port provides connection for a Cable/ADSL modem. The WAN port also supports Auto-MDIX, which eliminates the need for crossover cables.

Load Default
INIT To reset the Wireless Routing Center to factory defaults, insert a straightened paper clip into the Load Default hole to press the button. Keep pressing and turn the Wireless Routing Center off and on. Wait for at least five seconds before you release the button. Then wait for the Wireless Routing Center to finish booting.

If you want to restore your customized settings after loading defaults, refer to the *System Configuration* section in Chapter 4, *Web Configuration*, for more information.

Indicators

Front Panel

The following illustration shows the front panel of the Wireless Routing Center:

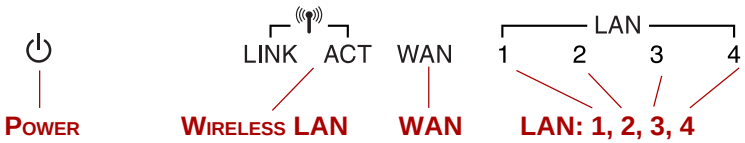


Figure 2-4 The indicators

LED Indicators

The Wireless Routing Center is equipped with eight LEDs on the front panel as described in the table below.

Table 2-1 Indicator conditions

LEDs	Function	Color	Status	Description
	Power	Green	Off	No power is supplied to the unit.
			Solid	Power is supplied to the unit.
LINK	Wireless Link	Green	Off	Wireless client is not associated.
			Blinking	Wireless client is associated. If “n” clients are associated, it blinks “n” times, off for 3 seconds and then repeats the blink pattern. If there are more than 10 clients associated, “n” will be 10.
ACT	Wireless Ready/ Activity	Green	Off	Wireless LAN interface is not initialized properly.
			Slowly blinking	Wireless LAN interface is initialized properly.
			Quickly blinking	Transmitting/receiving packets on Wireless LAN interface.
WAN	WAN Port Status	Green	Off	Power is off or no broadband device is connected.
			Slowly blinking	Broadband device is connected.
			Quickly blinking	Transmitting/receiving packets on the WAN port.
LAN 1-4	LAN Port Status	Green	Off	Power is off or no Ethernet device is connected.
			Slowly blinking	Ethernet device is connected.
			Quickly blinking	Transmitting/receiving packets on the LAN port.

Stand

A stand lets you install the Wireless Routing Center in an upright position on a desk.

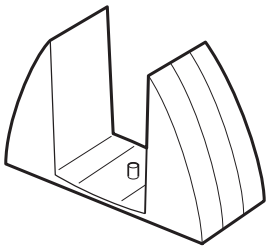


Figure 2-5 The stand

Screws for wall mount

Two screws are supplied to secure the Wireless Routing Center to a wall.

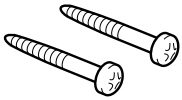


Figure 2-6 The two screws for wall mount

AC adapter and power cord

The AC adapter converts AC power to DC power and reduces the voltage supplied to the Wireless Routing Center. It can automatically adjust to any voltage from 100 to 240 volts and to a frequency of either 50 or 60 hertz, enabling you to use the Wireless Routing Center in almost any country/region.

> ***CAUTION:*** *Always use the correct AC adapter to avoid the risk of fire or damage to your Wireless Routing Center. The current rating for the Wireless Routing Center is 2.0 amperes.*

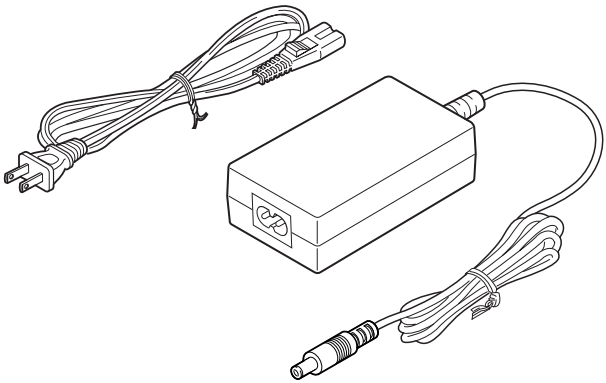


Figure 2-7 The AC adapter and power cord

Setup

This chapter describes how to position your Wireless Routing Center for wireless data exchange and how to connect cables.

The figure below shows an example of connections in a LAN and a LAN connection to the Internet.

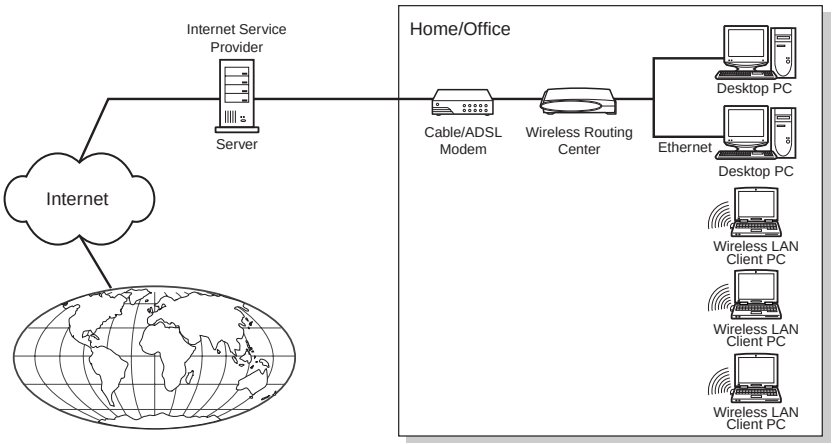


Figure 3-1 Network connections

Mounting

The Wireless Routing Center can be used either vertically or horizontally on a desk or hung on a wall.

NOTES: *1. Place the device close to a power outlet if possible.*

2. Avoid placing the device in places where people may walk on the cables. Also keep it away from direct sunshine or heat sources.

3. Place the device on a flat and stable stand.

Vertical mounting

To install the Wireless Routing Center upright on a desk, use the stand provided as an accessory.

1. Align the peg on the stand with the hole in the Wireless Routing Center and fit the Wireless Routing Center into the stand.

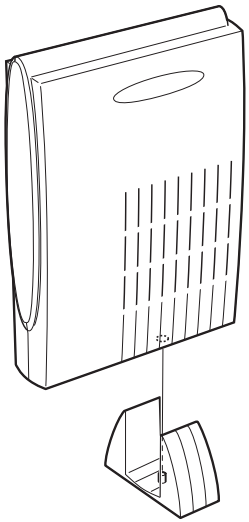


Figure 3-2 Installing the Wireless Routing Center in its vertical stand

2. Set the Wireless Routing Center upright.

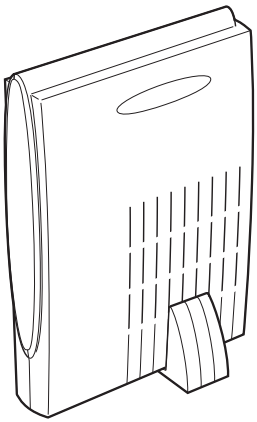


Figure 3-3 The Wireless Routing Center's upright position in a stand

Horizontal mounting

Four rubber pads protect the back of the Wireless Routing Center. Lay it on a flat surface with the pad side down.

Wall mounting

To install the Wireless Routing Center on a wall, secure it to with two screws provided with the Wireless Routing Center.

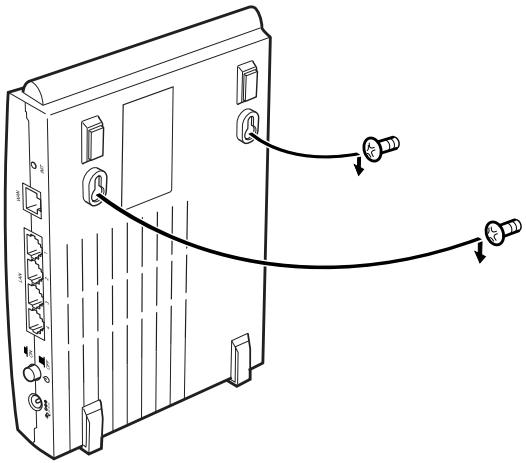


Figure 3-4 Mounting the Wireless Routing Center on a wall

AC adapter

Follow the steps below to connect the AC adapter.

1. Connect the power cord to the AC adapter.
2. Connect the AC adapter to the DC IN jack on the back of the Wireless Routing Center.
3. Connect the power cord to an electrical outlet (100 to 240 VAC).

CAUTION: *Use the adapter supplied with the Wireless Routing Center. Connecting the wrong adapter could damage the Wireless Routing Center. TOSHIBA assumes no liability for any damage in such case.*

Follow the order of 1, 2, 3 as shown in the figure below when you connect the AC adapter. Reverse the order when you disconnect.

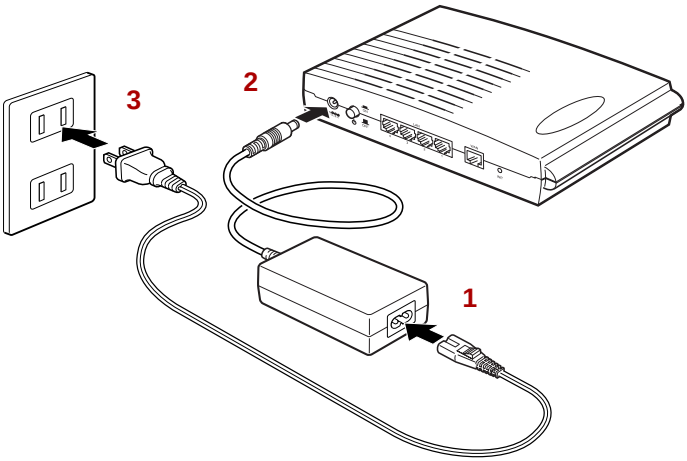


Figure 3-5 Connecting the AC adapter

Connecting the Wireless Routing Center

Prior to connecting the hardware, make sure to power off your Ethernet device, Cable/ADSL modem and Wireless Routing Center. Then follow the steps below to connect the related devices.

> ***CAUTION:*** *The computer must be configured properly before connecting to a LAN. Logging onto a LAN using the computer's default setting could cause a malfunction in LAN operation. Check with your LAN administrator regarding set-up procedures.*

1. Connecting your computer to the LAN port.

   Attach one end of the Ethernet cable with RJ-45 connectors to your hub, switch or a computer's Ethernet port, and the other end to one of the LAN ports of your Wireless Routing Center.

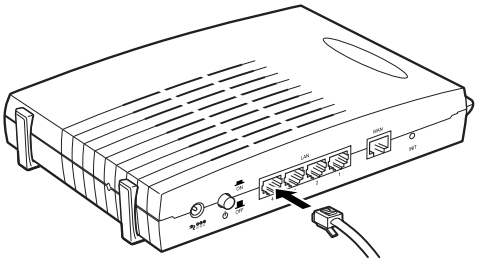


Figure 3-6 Connecting the LAN port

2. Connecting Cable/ADSL modem to the WAN port.

   Connect the Ethernet cable attaching to your Cable/ADSL modem to the WAN port of your Wireless Routing Center.

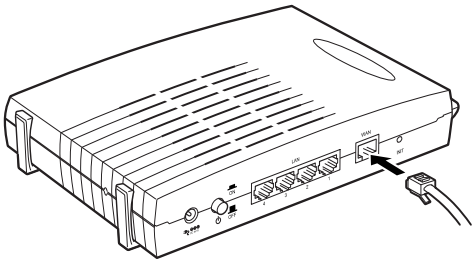


Figure 3-7 Connecting the WAN port

3. Connecting the power adapter.

   Connect the single DC output connector of the power adapter to the power jack on the side of the Wireless Routing Center. Then connect the supplied power cord to the power adapter and the other end to an AC outlet.

4. Turn on the power switch.

Setting up the Ethernet/Wireless LAN client

To access the Wireless Routing Center via Ethernet or wireless network, you must properly configure the network settings of your Ethernet or wireless client computer. As the Wireless Routing Center is configured with the default IP address of 192.168.10.1 and subnet mask of 255.255.255.0, and its DHCP server is enabled by default, you can configure your computer's TCP/IP settings as one of the following:

1. To use dynamic IP: Set your computer to be DHCP client to accept the dynamic IP from the router.
2. To use static IP: Set the IP address as 192.168.10.x (x is between 2 and 254), subnet mask as 255.255.255.0 and the gateway as 192.168.10.1 to be on the same subnet with the router.

This section describes how to configure your computer to be a DHCP client for initial connection to the Wireless Routing Center. If you have modified the Wireless Routing Center's network setting, your LAN/Wireless LAN clients should make appropriate changes in order to make a successful connection.

Setting up Ethernet client

To access the Wireless Routing Center via Ethernet, make sure your computer is equipped with an Ethernet network card and has an appropriate network card driver and TCP/IP installed.

NOTES: *1. If TCP/IP protocol is not installed on your computer, refer to Windows documentation for installation instructions.*

2. For initial verification, connect only one computer directly to an Ethernet port on the Wireless Routing Center, not through a hub. Connecting more than one computer may cause setting errors.

For Windows XP

1. From the **Start** menu, point to **Connect To** and then click **Show all connections**.

2. Right-click the **Local Area Connection** icon and then click **Properties**.
3. In the **General** window, highlight **Internet Protocol (TCP/IP)** and then click **Properties**.
4. Enable **Obtain an IP address automatically** and then click **OK**.

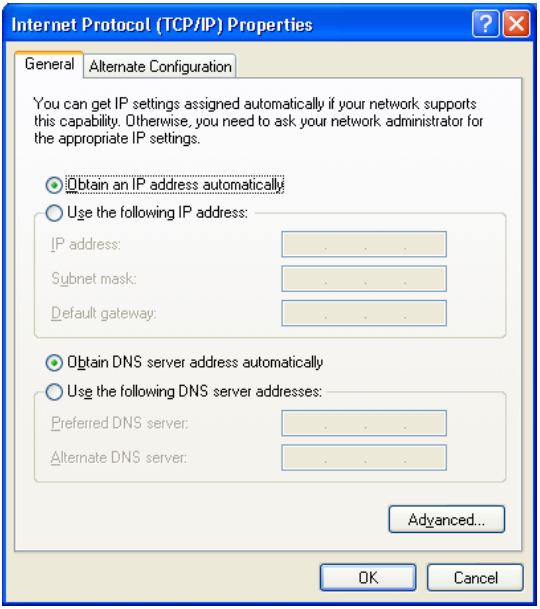

Internet Protocol (TCP/IP) Properties
General
Alternate Configuration
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
Subnet mask:
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Advanced...
OK
Cancel

Figure 3-8 Obtain an IP address automatically

Checking/Renew IP Address under Windows XP

The following steps help you verify that your network adapter gets an IP address within the DHCP IP pool range (192.168.10.100 ~ 192.168.10.150 by default) of the Wireless Routing Center. If not, you may need to renew the IP information.

1. Click **Run** from the **Start** menu to open the **Run** dialog box.
2. Type **cmd** in the dialog box and then click **OK**.
3. At the prompt, type **ipconfig** to see the IP information from DHCP server.
4. If you want to get a new IP address, type **ipconfig /release** to release the previous IP address and then type **ipconfig /renew** to get a new one.

For Windows 2000

1. From the **Start** menu, point to **Settings** and then click **Network and Dial-up Connections**.
2. Right-click the **Local Area Connection** icon and then click **Properties**.
3. In the **General** window, highlight **Internet Protocol (TCP/IP)** and then click **Properties**.
4. Enable **Obtain an IP address automatically** and then click **OK**.

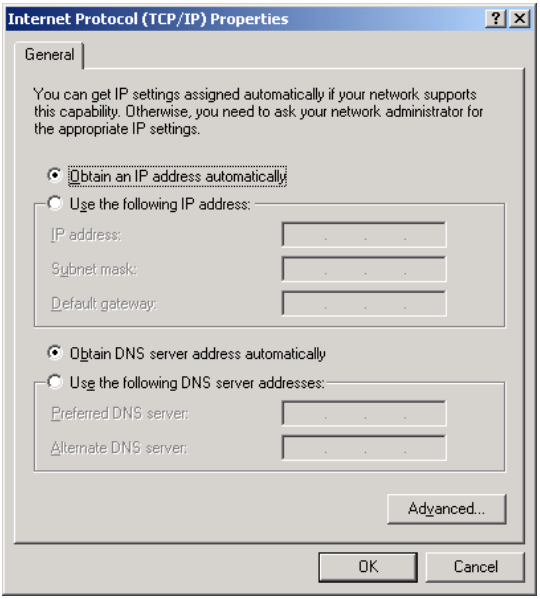

Internet Protocol (TCP/IP) Properties
General
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
Subnet mask:
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Advanced...
OK
Cancel

Figure 3-9 Obtain an IP address automatically

Checking/Renew IP Address under Windows 2000

To check if your network adapter gets an IP address within the DHCP IP pool range (192.168.10.100 ~ 192.168.10.150 by default) of the Wireless Routing Center, follow the related description under the Windows XP section. The procedures are the same.

For Windows 98/ME

1. Click the **Start** menu, point to **Settings** and click **Control Panel**.
2. Double-click the **Network** icon.
3. In the **Configuration** window, highlight **TCP/IP protocol** for your NIC and click **Properties**.
4. In the **IP Address** window, select **Obtain an IP address automatically**. Then click **OK**.

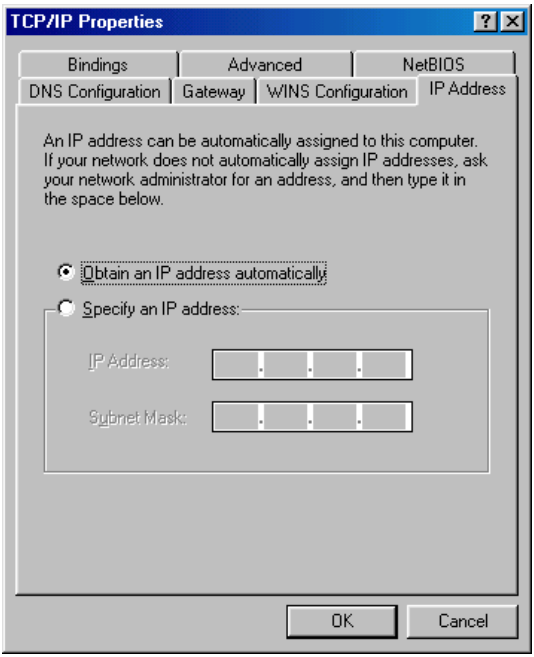

TCP/IP Properties
Bindings
Advanced
NetBIOS
DNS Configuration
Gateway
WINS Configuration
IP Address
An IP address can be automatically assigned to this computer. If your network does not automatically assign IP addresses, ask your network administrator for an address, and then type it in the space below.
Obtain an IP address automatically
Specify an IP address:
IP Address:
Subnet Mask:
OK
Cancel

Figure 3-10 Obtain an IP address automatically

5. If your network settings is changed, you will be prompted with the **System Settings Change** dialog box. Click **Yes** to restart your computer.

Checking/Renew IP Address under Windows 98/ME

The following steps help you verify if your network adapter gets an IP address within the DHCP IP pool range (192.168.10.100 ~ 192.168.10.150 by default) of the Wireless Routing Center. If not, you may need to renew the IP information.

1. From the **Start** menu, click **Run** to open the **Run** dialog box.
2. Enter **winipcfg** in the dialog box and then click **OK**.
3. Select the Ethernet or Wireless LAN adapter from the drop-down list to show the IP address. If necessary, click **Release** and then **Renew** to get a new IP address.

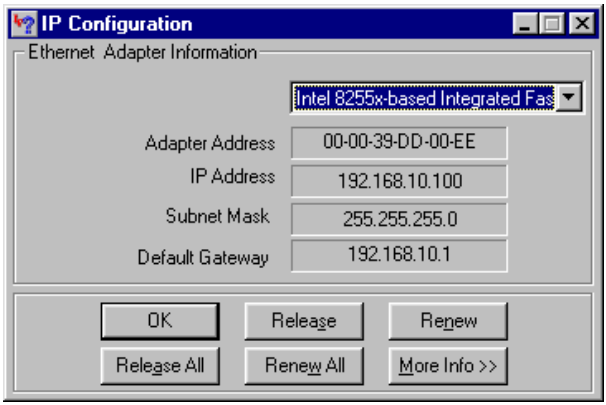


Figure 3-11 Specify an IP Configuration

Setting up Wireless client

You can also choose to access the Wireless Routing Center via a wireless client, whether for configuration purposes or sharing network resources and an Internet connection. To get your wireless client connected to the Wireless Routing Center, verify the following:

1. Make sure your computer is equipped with a Wireless LAN adapter and has an appropriate Wireless LAN card driver/utility and TCP/IP installed.
2. Set the Wireless LAN client to obtain a dynamic IP address from the Wireless Routing Center.

   The procedures are the same as described above. The only difference is that you are configuring the TCP/IP associated with your Wireless LAN card.

3. Verify that your Wireless LAN setting is identical to the router's default wireless settings.

Checking Connection with the Wireless Routing Center

You can use the Ping command to verify whether or not your Ethernet/Wireless client is connected to the Wireless Routing Center.

To execute ping command, open a DOS window and ping the IP address of the Wireless Routing Center at the DOS prompt. For example:

ping 192.168.10.1

If the following response occurs:

```
Reply from 192.168.10.1 bytes=32 time=100ms TTL=255
```

Then the connection between the Wireless Routing Center and the network is OK.

If you get a failed ping with the response of:

```
Request time out
```

Then the connection has not been made. Verify your network setting are correct. For Ethernet client, also check the cable between the Wireless Routing Center and the computer.

Web Configuration

After you have configured your system as described in Chapter 3, *Setup*, you can proceed with the initial configuration described in this chapter.

You can manage the Wireless Routing Center through a Web browser-based manager. To configure the Wireless Routing Center via Web browser, at least one properly configured computer must be connected to the network and reside on the same subnet as the Wireless Routing Center. The Wireless Routing Center comes with the default IP address of 192.168.10.1 and subnet mask of 255.255.255.0. The DHCP Server is enabled by default. You can also use the TOSHIBA WRC Finder program on the TOSHIBA Wireless Routing Center WRC-1000 Utility CD-ROM to open the Wireless Routing Center's Web Configuration page.

NOTES:

1. *If data is being transmitted while you are changing settings, transmission will be interrupted when you click* **Apply**.
2. *The DHCP server function is enabled before the Wireless Routing Center is shipped. If the LAN has other DHCP servers, the DHCP server function of the Wireless Routing Center must be disabled.*
3. *You will need Internet Explorer version 5.0 or higher.*
4. *If your browser is set to allow you to use a Proxy on your LAN, you will not be able to display the Wireless Routing Center set-up page. In this case, follow the steps below.*
   a. *Open the* **Start** *menu and open the* **Control Panel**.
   b. *Click* **Network and Internet Connections**.
   c. *Click* **Internet Options**.
   d. *Select the* **Connections** *tab and click* **LAN Settings**.
   e. *Clear the checkbox for* **`Use a proxy server for your LAN (These settings will not apply to dial-up or VPN connections)`**.
   f. *Click* **OK**.

Accessing Web Configuration Page

> ***NOTE:*** *Connect the computer running WRC Finder to the Wireless Routing Center by cable. You should not use a wireless connection.*

The computer running WRC Finder must be on the same subnet as the Wireless Routing Center in order to display the Wireless Routing Centers in a list. If you want to change a setting in a Wireless Routing Center, double-click the Wireless Routing Center you want to change. Your Web browser will start and display that Wireless Routing Center's Web Confirmation Page.

> ***NOTE:*** *If you know the IP address of the Wireless Routing Center you want to set, you can enter* **http://????????????/** *in your Web browser and go directly to the Web Confirmation Page. (***?** *specifies the IP address of the Wireless Routing Center. The default value is 192.168.10.1)*

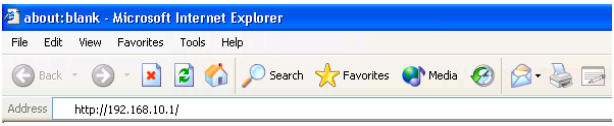


Figure 4-1 Web Browser

1. Follow the steps below to start TOSHIBA WRC Finder.
   1) Load the TOSHIBA Wireless Routing Center WRC-1000 Utility CD-ROM in the set-up computer.
   2) Use Windows Explorer to locate and copy the file **WRC_FIND.exe** to the computer's hard disk.

3) Double-click the copied file **WRC_FIND.exe** to start the WRC Finder.

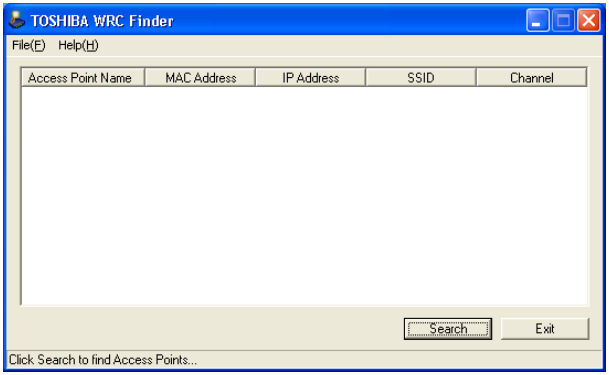


Figure 4-2 WRC_FIND.EXE

2. Follow the steps below to find Wireless Routing Center.

1) A dialog box will be displayed asking you if you want to search for Wireless Routing Centers.

Figure 4-3 Confirmation window

2) If you click **No**, WRC Finder will do nothing. At this point, you can still continue by clicking **Search**.

3) If you click **Yes**, the Wireless Routing Center search will begin. In about five seconds, a list of Wireless Routing Centers will be displayed.

4) When the WRC Finder locates a Wireless Routing Center, the following information will be displayed:

Access Point Name: Wireless LAN's Access Point Name

MAC Address: Access Point's MAC Address

IP Address: WRC-1000's IP Address

SSID: SSID

Channel: The channel that is being used.

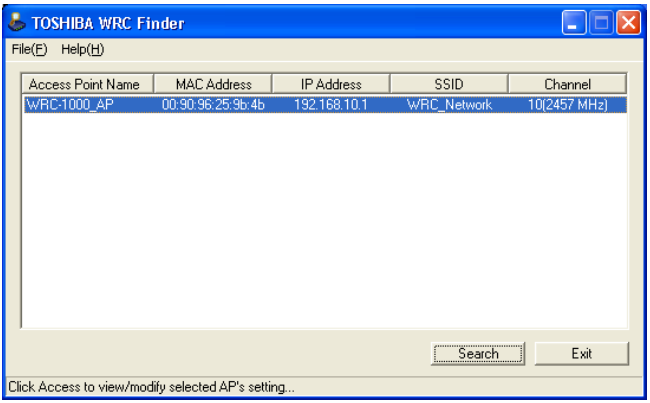


Figure 4-4 WRC information

5) If no Wireless Routing Center is found, the Confirm dialog box is displayed again.

3. Open the Web Configuration page.

Double-click the Wireless Routing Center you want to set. The Web browser will start and display the selected Wireless Routing Center's Web Configuration Page. A Password input window will also be displayed. If the Password input window does not appear, see the section, *Configuration window*, in Chapter 5, *Troubleshooting*.

After connecting to the Wireless Routing Center, you will be prompted to enter username and password. Leave the username **admin** and enter the default password of **password**.

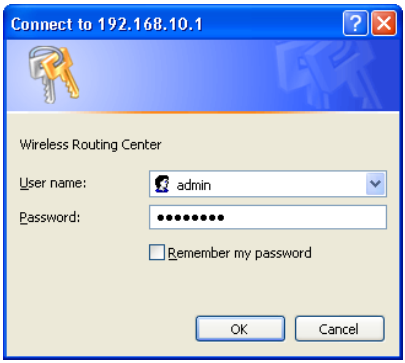


Figure 4-5 Password window

After you login, the **Overview Configuration** page of the Wireless Routing Center will be displayed. From this point on, the Wireless Routing Center will act as a Web server sending HTML pages/forms on your request. You can click the menu options at the left side to start your configuration task.

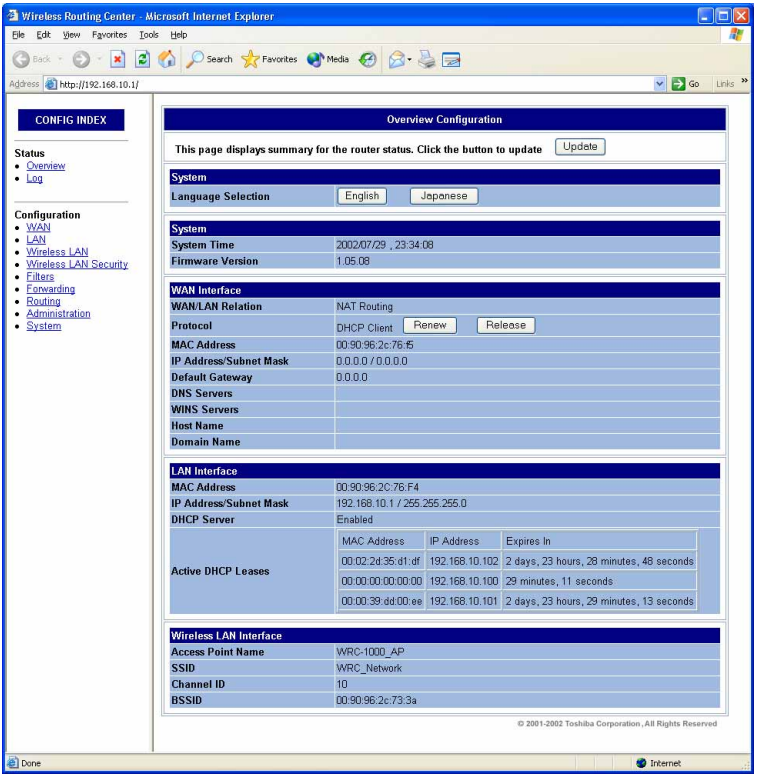


Figure 4-6 Configuration window

When you make settings with the Web configuration utility, fields related to a selected option will be displayed to avoid conflicting setting. The utility also displays an error message if you enter an invalid value.

To enable your settings

After you have customized the settings, click the **Apply** button. The Wireless Routing Center will begin registering the settings. You will be prompted to wait for a few seconds. During this process, it is important not to turn the Wireless Routing Center OFF or ON. The Wireless Routing Center could be damaged.

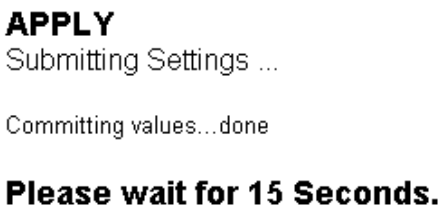


Figure 4-7 Apply changes

After the settings have been registered, the screen will return to the previous page. You can then proceed with other configuration tasks.

Viewing system overview and log

Overview Configuration

Clicking the **Overview** link in the Status menu will display the **Overview Configuration** page which shows the basic information of your Wireless Routing Center, including the system, WAN/LAN interface and Wireless LAN interface information. In addition to the general information, this page contains the following elements:

Update button: Click the **Update** button on the top to update the overall status.

Language Selection: Lets you select the Web browser's encoding language: **English** or **Japanese**.

WAN Interface: Information and buttons differ according to whether the router's WAN/LAN relation is DHCP Client, PPPoE Client or Manual Config.

PPPoE Client: Displays the PPPoE client information. The **Connect/Disconnect** buttons let you manually launch/terminate your PPPoE session.

DHCP Client: Displays the DHCP client information. To update the IP information assigned to the router's WAN port, click **Release** and then click **Renew**.

Manual Config: Displays the WAN port information you manually specified.

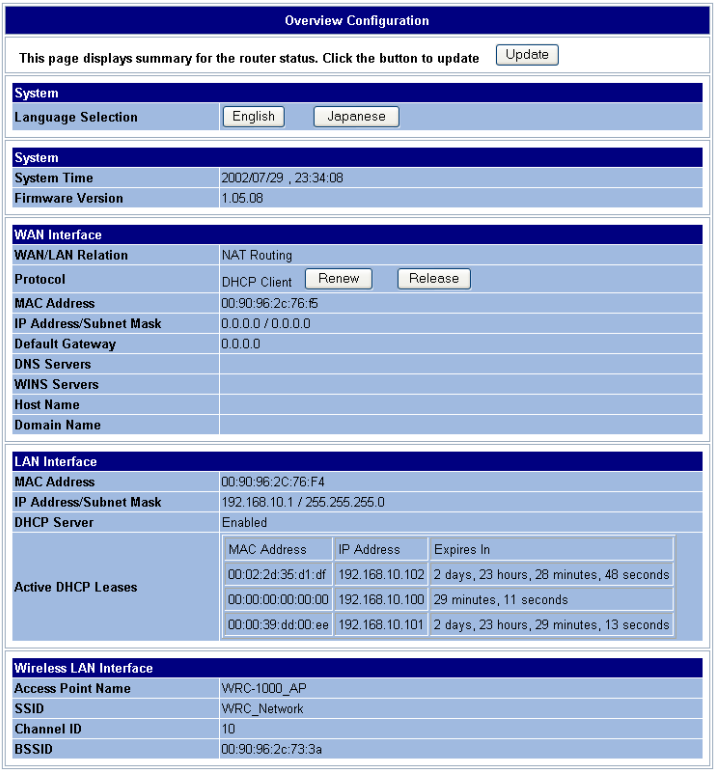


Figure 4-8 Overview Configuration

Filter Log

If filter feature is enabled, you can click the **Log** link in Status menu to display the filter activity log. See *Viewing Filter Log* for more information on log category.

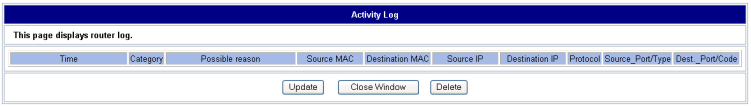


Figure 4-9 Activity Log

Configuration for NAT Routing Mode

Before you configure your Wireless Routing Center, you must decide whether to configure the Wireless Routing Center as a router or as a bridge. This section describes only how to set up the Wireless Routing Center as a router. For instructions on bridge configuration, refer to the section, *Configuration for Bridge Mode*, in this chapter.

When operating as a router, the Wireless Routing Center communicates with your ISP through the WAN port. Depending on the connection type offered by your ISP, you may get the WAN IP address by one of the following means:

- **DHCP Client:** In this connection type, your router acts as a DHCP client and requests IP information from the DHCP server on the ISP side. Select this option if your ISP assigns you a dynamic IP address each time you log on.
- **PPPoE Client:** Some ISPs use a PPPoE session to connect to their clients. If this is the case, you should enable this option and finish the PPPoE Client settings. The WAN port of the Wireless Routing Center will be assigned a public IP address from your ISP's server.
- **Manual Config:** If your ISP assigns you a fixed IP address, you should select this option and manually enter the IP information provided by your ISP.

  The configuration items displayed depend on your connection type. Ask your ISP which option applies to you and obtain the information you need for correct configuration. After you have done so, proceed with the following sections.

WAN Configuration for NAT Routing Mode

Click **WAN** in the configuration menu to enter the WAN Configuration page and carry out the procedures below.

Part 1. Configuring general settings

1. In the **WAN/LAN Relation** field, select the **NAT Routing** option.

   This option allows the Wireless Routing Center to act as a router and use the built-in NAT function to translate your multiple private IP addresses to a single public IP address. However, only outgoing requests are allowed to pass through the Wireless Routing Center unless you specify otherwise. Outside users cannot see your private local IP addresses. This protects your home or business network from outside intruders.

2. In the **Protocol** field, select a protocol type according to the connection type offered by your ISP.

3. If required, in the **MAC Address** field, enter your network adapter's MAC address in the format of xx:xx:xx:xx:xx:xx. Otherwise keep the default values.

   This field allows you to copy a network adapter's MAC address to the WAN port of the Wireless Routing Center. Some ISPs use the MAC address of the NIC, which was connected to the Cable/ADSL modem, for static mapping. This would give you the same IP address each time the Cable/ADSL modem requests an IP address for the Ethernet port. If this is the case, this feature removes the need of asking your ISP to change the registered MAC address. You can still use the same IP you were given for the router's WAN port.

4. In the **Host Name** field, you can supply a host name for the Wireless Routing Center if this is required by your ISP. Some ISPs only respond to a DHCP request with a valid Host Name. If a host name is not necessary for your ISP, leave it blank.

Part 2. Configuring protocol settings

Proceed to the section corresponding to the connection type you selected above.

▶ DHCP Client

If DHCP Client is your option, no other configuration is needed. Click **Apply** to end your WAN settings. After the connection to ISP is established, the information provided by your ISP will be displayed in the **DHCP client** group.

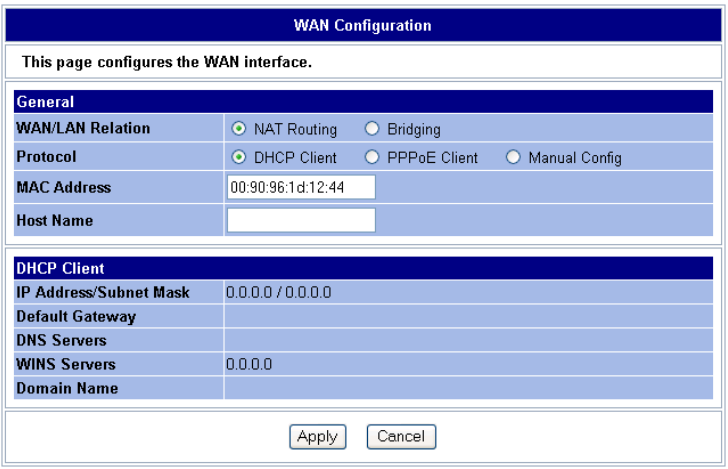


Figure 4-10 WAN Configuration-DHCP Client

▶ PPPoE Client

If PPPoE Client is your option, configure these fields as required by your ISP.

PPPoE Connection Status: This item is not configured. It displays whether the connection is up or down.

Username/Password: Enter the user name and password provided by your ISP for logging onto the Internet.

Authentication Mode: Usually, you should select **Auto**. When **Auto** is selected, the Wireless Routing Center automatically determines whether the mode is **PAP** or **CHAP** and makes the connection. If a connection cannot be made with the **Auto** setting, check with your ISP and set either **PAP** or **CHAP**.

Connection Mode: Select **Keep Alive** or **Connect on Demand**.

Keep Alive: This feature will keep your PPPoE-enabled Internet connection always open. This is done by sending echo requests periodically to the ISP to prevent the connection from being terminated by the ISP.

Connect on Demand: If enabled, the router will trigger a PPP session for connection to the Internet if any client computer on your LAN sends a request for Internet access. However, the router automatically disconnects the PPP session after the WAN connection has been idle for the amount of time specified in the **Max Idle Time** box. If your Internet account is billed based on the amount of time of your Internet connection, you can reduce charges by enabling this option. Enter an idle time value best suited for your network.

MTU/MRU: Allows you to adjust the Maximum Transmission/Receive Unit in bytes for the WAN interface. You may need to adjust the values to a smaller size if the servers of your ISP do not support full-size frame packets. Packets larger than the specified values will be fragmented, which could hurt performance.

It's better not to modify the MTU/MRU settings unless your ISP advises you to.

After you finish the WAN settings, click **Apply** to submit your changes.

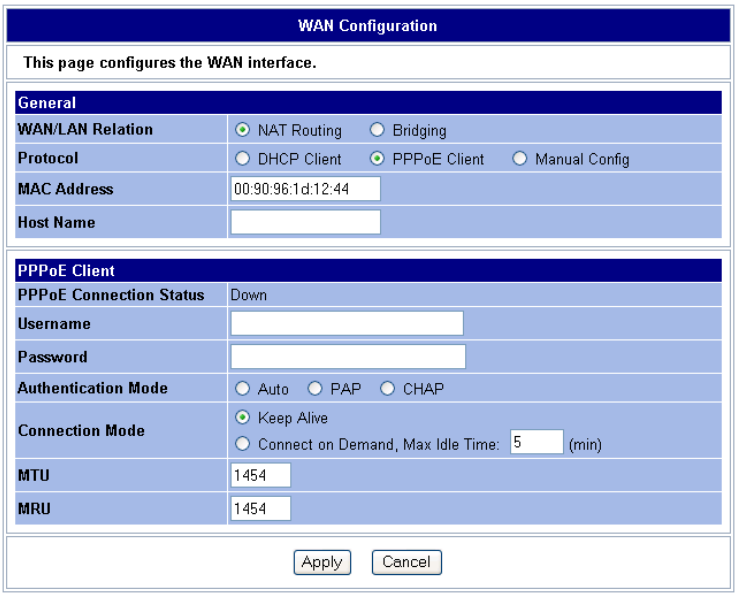


Figure 4-11 WAN Configuration-PPPoE Client

▶ Manual Config

If Manual Config is your option, configure these fields as required by your ISP.

IP Address/Subnet Mask: Enter the fixed IP address and subnet mask given by your ISP. The default values are 0.0.0.0/0.0.0.0.

Default Gateway: The IP address of the default gateway of the router is the IP that the Wireless Routing Center first contacts to communicate with the Internet. The default is 0.0.0.0.

DNS Servers: Specifies the IP address of the Domain Name Server. Your LAN side DHCP clients use the DNS to map a domain name to its corresponding IP address and vice versa. Up to three DNS servers are allowed.

WINS Servers: Optional for Windows Internet Names Service. Enter the IP addresses of WINS servers if required.

Domain Name: Optional. Allows you to supply a host and domain name for the Wireless Routing Center.

After you finish the WAN settings, click **Apply** to submit your changes.

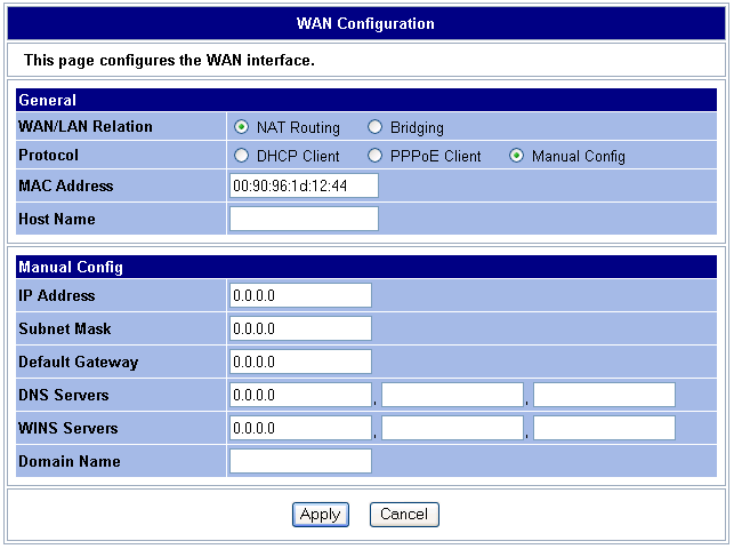


Figure 4-12 WAN Configuration-Manual Config

LAN Configuration for NAT Routing Mode

The Wireless Routing Center communicates with a LAN through a LAN port. The LAN configuration page lets you define the private IP address and DHCP server settings over the LAN interface.

1. In the **`Manual Config > IP Address/Subnet Mask`** field, enter the IP address and subnet mask for the LAN port.

   The default LAN port IP address is 192.168.10.1 and the subnet mask is 255.255.255.0. Note that if you change the private IP address and apply the changes, the computer from which you configure the router will lose communication to the router. To reconnect, you will need to renew the IP address of the computer or change to an IP address compatible with the new LAN port IP address.

2. In the **`DHCP Server > Service`** field, select whether to enable DHCP service on the LAN port.

The Wireless Routing Center implements a built-in DHCP (Dynamic Host Configuration Protocol) server on its LAN interface, which dynamically assigns IP addresses to DHCP clients on the LAN/Wireless LAN. The DHCP server also provides a default gateway (the router's LAN IP address) and DNS addresses for DHCP clients to access the Internet. The DHCP function spares you the hassle of manually assigning a fixed IP address to each computer on the LAN/Wireless LAN. If your network already has a DHCP server do not enable this function. DHCP server is enabled by default.

NOTE: *Only one DHCP server can run on one LAN. If you decide to enable DHCP on this router, remember to disable the DHCP function of the other device.*

If you disable DHCP, no further configuration is required for the Wireless Routing Center. Click **Apply** to submit your changes. If you enable DHCP, proceed to the next step.

NOTE: *Set the DNS Server IP address of the computer connected to the LAN port to the IP address of the LAN's Wireless Routing Center.*

3. If DHCP server is enabled, enter the fields below:

   DHCP Lease Time: Specify the time that a network device can lease a private IP address before the DHCP server reassigns the IP address.

IP Pool Range: Specify the starting and ending IP address of the IP address pool. Whenever a network device requests an Internet session, the router will allocate an unused IP address from this pool and lease it to the device for a specified amount of time.

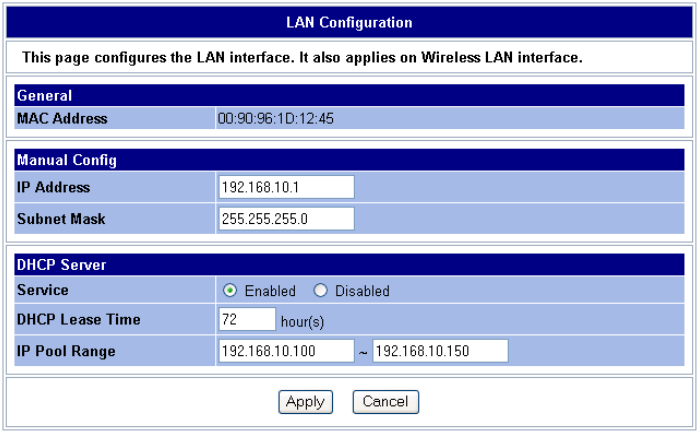


Figure 4-13 LAN Configuration in Router Mode

Viewing Current DHCP Assignments

When the DHCP server function is enabled for your LAN, the Wireless Routing Center keeps a record of any computer (either Ethernet or Wireless node) that has leased an IP from the specified IP pool. The DHCP lease table is displayed under **`Overview > LAN Interface`**:

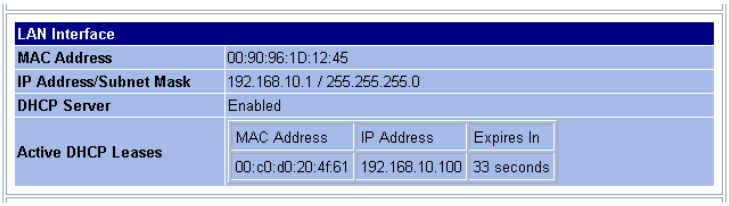


Figure 4-14 DHCP Lease Table

Configuration for Bridge Mode

A bridge connects two or more LANs, and it bases the forwarding decision on the MAC address. In Bridge mode, filters, forwarding and routing do not apply. To set up the bridge mode, perform the procedures below.

Part 1. Enable bridging function

Go to the WAN configuration page and select the **Bridging** option in the **`WAN/ LAN Relation`** field and then click **Apply** to commit the changes.

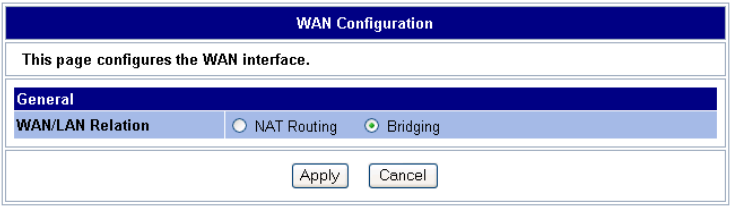


Figure 4-15 Enabling Bridging

Part 2. LAN configuration

In the **`General > Protocol`** field, select **Manual Config** or **DHCP Client** as required.

DHCP Client: Select this option if your network already has a DHCP server that assigns IP to this bridge. If enabled, no further configuration is needed since the DHCP server will pass the required IP information. Click **Apply** to submit your changes.

> ***NOTE:*** *After registering the setting, your configuring computer may lose connection to the Wireless Routing Center. To reconnect, you will need to make sure the computer uses an IP address in the same subnet as the Wireless Routing Center.*

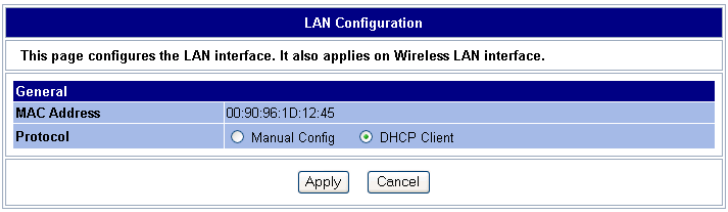


Figure 4-16 Bridge Mode-DHCP Client

Manual Config: If enabled, manually enter the IP address, its subnet mask and default gateway in **`IP Address/Subnet Mask/Default Gateway`** fields.

> ***NOTE:*** *To reconnect after committing this setting, you will need to make sure the computer uses an IP address in the same subnet as the manually entered IP.*

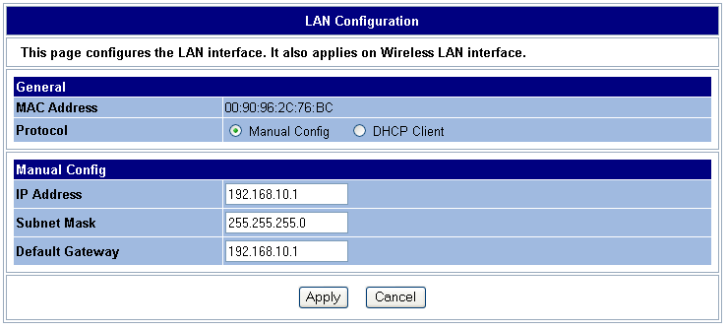


Figure 4-17 Bridge Mode-Manual Config

Wireless LAN Configuration

The Wireless Routing Center implements Access Point capability which connects wireless clients to a wired LAN. It allows wireless nodes to access network resources and share the broadband Internet connection. With the default values, the router (Access Point) can be easily associated by a wireless client. We suggest that you customize the wireless settings to prevent unauthorized association.

> ***NOTE:*** *One Wireless Routing Center can accommodate multiple computers. However, optimal LAN operation can be maintained with up to 10 computers.*

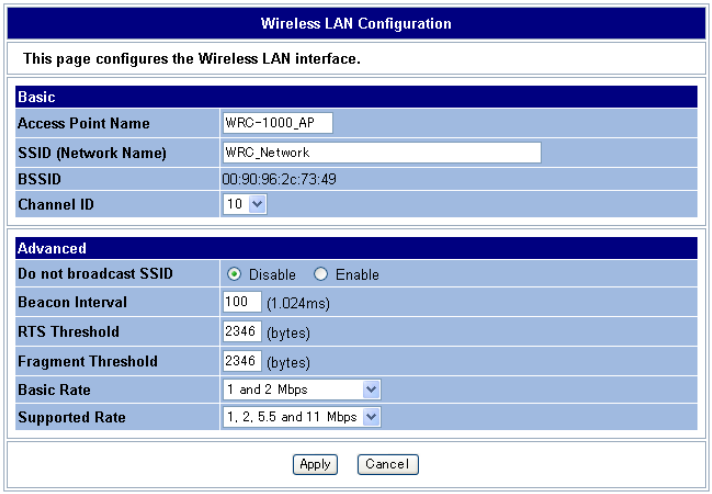


Figure 4-18 Wireless LAN Configuration

Basic

Access Point Name: The name used to identify the Access Point.

SSID (Network Name): Service Set ID. It uniquely identifies the logical network domain name of your Wireless LAN. The default value is WRC_Network.

BSSID: Basic Service Set ID. It is the MAC address of the Access Point. It can be used to identify the AP, especially when wireless stations roam among different APs which all share the same SSID.

Channel ID: The radio frequency used for communication. Available channels vary according to the regulations in your area. Select a channel out of the available channels or use the default channel.

Advanced

Do not broadcast SSID: An AP will periodically broadcast its **SSID** to allow the wireless clients to recognize its presence. However, this creates a security hole since any wireless station with SSID set to "any" may associate with your AP. Enabling this option is recommended in order to have your AP accept only stations whose **SSID** is the same as its own.

Beacon Interval: Defines the periodic intervals at which the 802.11 Wireless LAN Access Point sends a beacon.

RTS Threshold: Request to send threshold. It specifies the packet size beyond which the AP invokes its RTS/CTS mechanism. Packets that exceed the specified RTS threshold trigger the RTS/CTS mechanism.

Fragmentation Threshold: It determines whether packets will be fragmented and at what size. On an 802.11 wireless LAN, packets that exceed the fragmentation threshold are fragmented into smaller units suitable for the circuit size. On the other hand, packets smaller than the wireless station's should be used to connect to your Access Point.

Basic Rate: Specifies the basic rate the wireless stations should use to connect to your Access Point.

Supported Rate: Allows the AP to automatically adjust the transfer speed to the rates you specified.

Wireless LAN Security

The Wireless Routing Center provides three types of wireless communication security.

- IEEE802.1x
- WEP (Wired Equivalent Privacy)
- Access Control

The combination of these three features provides a high level of security for Wireless LAN transmissions.

For details of IEEE802.1x functions refer to Appendix B, *802.1x*.

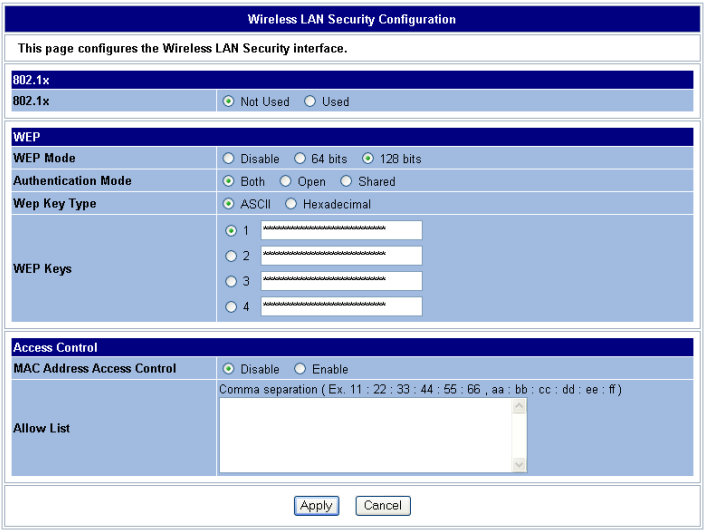


Figure 4-19 Wireless LAN Security

802.1x

802.1x: Specify whether to use the 802.1x function. The options are **Not Used** and **Used**.

Wep Key Distribution: Specify whether to dynamically distribute the WEP key. This radio button will appear when the 802.1x function is used.

Key Length: Specify the length of the WEP key to be distributed. This radio button will appear when the 802.1x function is used.

WEP

WEP Mode: WEP (Wired Equivalent Privacy) is an authentication algorithm that encrypts your data and protects your Wireless LAN against eavesdropping.

WEP is disabled by default. If you want to protect your data when it is transferred from one station to another, you should enable this security option. For security concerns, we strongly recommend that you enable the WEP function.

To enable WEP, select **64 bits** or **128 bits** as the encryption algorithm. The higher the number of bits, the greater the complexity and the security of the encryption.

Authentication Mode: Authentication is a process in which the AP validates whether wireless clients are qualified to access the AP's service. A wireless client must be validated before it can associate with an AP. The IEEE802.11 defines two types of algorithms in authentication: "open" and "shared" key.

With open key, the authentication is done through a pseudo process, accepting all kinds of requests, mainly used in cases where connectivity is more important than security. Shared key, on the other hand, utilizes WEP capability to further verify if the wireless client is authorized to share this AP's resource. If the client has the wrong key or no key, it will fail authentication and will not be allowed to associate with the AP.

If WEP is enabled …

Select your authentication mode: **Both, Open** or **Shared**. **Both** allows the wireless client to use either authentication method. The authentication type must be the same on the Access Point and wireless stations to be able to communicate.

If WEP is disabled …

If WEP is disabled, the Authentication Mode is automatically set to **Open**.

WEP Key Type and **WEP Keys:** For flexibility, you can enter the WEP keys in either **ASCII** or **Hexadecimal** format. Select a format and then enter the key values in the **WEP keys 1-4** fields. All four fields need to be entered.

Note that when using Hexadecimal format, only digits 0-9 and letters A-F, a-f are allowed. Valid key length for each encryption type is as below.

	HEX Format	ASCII Format
64 bit	10 hexadecimal digits	5 ASCII characters
128 bit	26 hexadecimal digits	13 ASCII characters

Aside from entering your WEP keys, you should select one of the four keys to encrypt the data before being transmitted. The AP always transmits data encrypted using this WEP key. The key number (1,2,3,4) is also transmitted. The receiving station will use the key number to determine which key to use for decryption. If the key value does not match with the transmitting station, the decryption will fail. To ensure successful decryption, have your wireless stations set identical key tables.

> ***NOTE:*** *All Wireless Stations must use identical encryption algorithm level and Key values (same key position in its key table) to ensure successful data transmission.*

Access Control

MAC Address Access Control: The Wireless Routing Center also supports authentication based on the MAC address of a wireless client. If this function is enabled, the AP will allow association by a client only if that client's MAC address matches an address in the **`Allow List`**.

To enable this function, select **Enable** option and enter the **MAC Address** of the Wireless LAN card in a Wireless LAN station to be allowed access to the Wireless Routing Center. A MAC address must be entered in 12 digits of hexadecimal, punctuated by a colon every 2 digits. MAC addresses must be separated by a comma. Spaces, tabs, and line feed are ignored. Example: 11:22:33:44:55:66, aa:bb:cc:dd:ee:ff

RADIUS Server

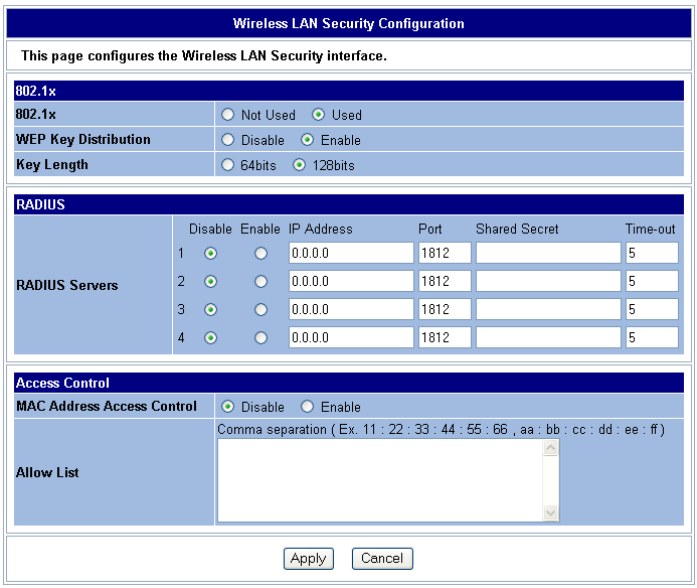


Figure 4-20 Wireless LAN Radius

This setting is used to validate wireless stations by **RADIUS servers**. Settings can be made for up to four RADIUS servers.

Enable/Disable: Use the radio buttons to disable or enable validation of wireless stations by RADIUS servers.

IP Address: Set the IP address of the RADIUS server.

Port: Set the port number of the RADIUS server.

Shared Secret: Set the shared secret of the RADIUS server. The shared secret is a password for communication between the access point and the RADIUS server.

Time-out: Set a time-out value in seconds. A maximum of five packets can be sent in the set interval.

Filters

When your Wireless Routing Center operates as a router, the built-in NAT function provides your LAN with Internet access via the single public IP of the WAN port. That means all network devices are allowed to access the Internet. Therefore, network security becomes an important issue and system administrators may need to build access controls to protect the network.

Filters serve as a basic security measure for your network. When the filter function is enabled, the Wireless Routing Center inspects all data packets received from the LAN and determines if packets are allowed to pass through the WAN port. Whether a packet is allowed to pass through, depends on whether it matches your filter rules and whether your filter type is Listed Pass or Listed Block.

Specifying IP Filter Rules

> ***NOTE:*** *If you make a mistake in Filter Rules, you might not be able to access the Internet.*

If you are going to specify your filter rules, follow the procedures below:

1. In the **General > Filter Type** field, select the action (**Listed Block** or **Listed Pass**) to be performed on the IP packets matching your filter rules.
2. In the four filter types, select whether to enable or disable each filter.
3. If a filter is enabled, enter the criteria in the fields provided. Click **More** to add more criteria if required. See the next section for more information.
4. Click **Apply** to register your changes.

Filter Types

When setting up filter rules, you can define the Filter rules based on the LAN computer's MAC address, IP address or the protocol type of the data packet. Each filter type is described below.

> ***NOTE:*** *Based on the OSI reference model, MAC Filters have higher priority than IP Filters while IP Filters have higher priority than Port Filters.*

MAC Filters: Specifies the MAC address of the LAN computer from which packets are allowed (or prohibited) to pass through the WAN port. Up to 12 entries are allowed.

IP Filters: Specifies the range of IP addresses of the LAN computers from which packets are allowed (or prohibited) to pass through the WAN port. You may enter the same address in both (IP Start and IP End) fields to define a single IP address. Up to 5 entries are allowed.

TCP Port Filters: Allows (or prohibits) LAN computers in the specified IP range to use TCP based service in the specified port range through the WAN port. You may enter the same address in both (IP Start and IP End) fields to define a single IP address. Up to 12 entries are allowed.

For example, to allow (or prohibit) a local computer 192.168.10.210 to use FTP service (using TCP port 20 and 21):

IP Start	IP End	Port Start	Port End
192.168.10.210	192.168.10.210	20	21

UDP Port Filters: Allows (or prohibits) LAN computers in the specified IP range to use UDP based service in the specified port range through the WAN port. You may enter the same address in both (IP Start and IP End) fields to define a single IP address. Up to 12 entries are allowed.

For example, to allow (or prohibit) local computers 192.168.10.140~192.168.10.150 to use ping service (using UDP port 53):

IP Start	IP End	Port Start	Port End
192.168.10.140	192.168.10.150	53	53

Filter Scenario of the Wireless Routing Center

When setting up your filter policies, note the filter scenario used by the router:

When Filter Type is Listed Block:

If all filters are disabled: No filter rule is specified to block any packet. All packets can pass through the WAN port. (Defaults)

If any filter is enabled: only the packets matching the specified rule are blocked; other packets can pass through the WAN port.

When Filter Type is Listed Pass:

If all filters are disabled: No filter rule is specified to allow any packet to pass. All packets are blocked.

If any filter is enabled: Only the packets matching the specified rule can pass; other packets are blocked.

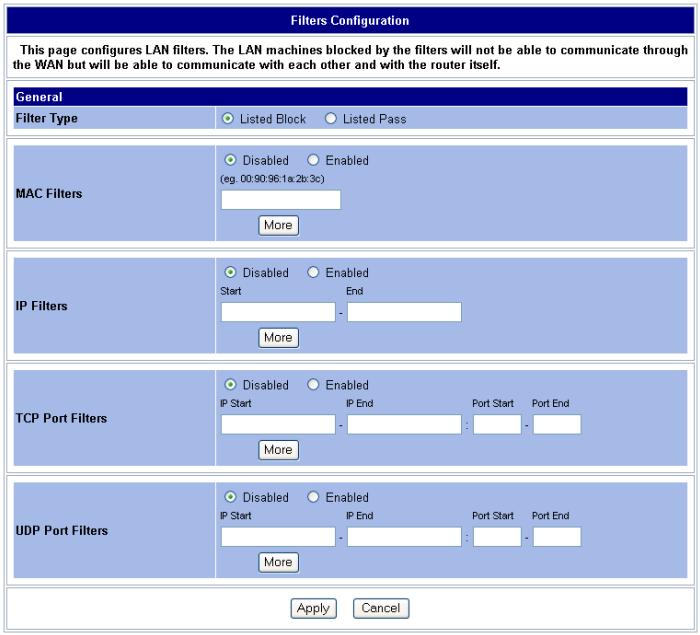


Figure 4-21 Filters Configuration

Viewing Filter Log

When the filter feature is enabled, the router will keep a record of the packets discarded. To view the firewall activity log, go to **`Status > Log`**. **`Activity Log`** is displayed with a maximum of 32 entries. Click the **Update** button to refresh the log with newly reported data. The log types are defined below.

Category	Possible reason
1	Blocked packets, from WAN side, by DoS (Deny of Service) protection mechanism.
2	Blocked packets, from LAN side, by MAC/IP/TCP/UDP filter.

Forwarding

This page allows you to configure the Forwarding and DMZ (De-Militarized Zone) features. Unlike Filter which governs outgoing traffic, Forwarding is used to provide external access to your local computers. This is commonly used when you have publicly accessible virtual servers on your local network.

By default, forwarding entry is empty and any external access to your LAN is blocked. Once you define a forwarding entry, incoming packets (identified by port number) that match your Forwarding criteria will be forwarded to the port range of the specified local computer. Otherwise packets are blocked. Forwarding protects your network from hazardous packets.

However, if you designate a DMZ sever, incoming packets that do not match the forwarding criteria will be redirected to the DMZ IP address. Forwarding has a higher priority than DMZ.

> ***NOTE:*** *The wrong Port Forwarding setting could allow unauthorized access to the LAN. Please be careful when you make Port Forwarding settings.*

Setting Up Forwarding Entries

To set up your forwarding entries, enter the following fields:

DMZ IP Address: DMZ setting allows a local computer to be exposed to the Internet. If you specify a DMZ host, all virtual service requests not specified in the Forwarding table are forwarded to the DMZ host.

TCP Port Forwards: In the first **Start** and **End** fields, define the port range for the incoming TCP service you want to forward. In the **IP Address** field, enter the IP address of the virtual server to which packets are forwarded. The **Start/ End** fields on the right side define the port range for the TCP service on the virtual server.

For example, the setting below allows access on virtual server 192.168.10.210 using FTP service.

Start	End	IP Address	Start	End
20	21	192.168.10.210	20	21

UDP Port Forwards: The configuration is the same as setting TCP Port Forwards, only that the entry applies to UDP service.

When the router gets outside TCP/UDP requests destined for the WAN port, it determines whether the services are allowed according to your forwarding settings. For example, if you do not specify FTP virtual service in the Forwarding table, incoming FTP requests (identified by port number in packets) are blocked or otherwise sent to the DMZ host (if specified). On the other hand, if an FTP forwarding entry has been set up, the FTP requests will be forwarded to the specified computer.

> ***NOTE:*** *If you set multiple forwarding entries, they will be used in order from the first entry. In the example below, incoming FTP requests will be sent to IP Address 192.168.10.220 not to 192.168.10.210.*

Start	End	IP Address	Start	End
20	25	192.168.10.220	20	25
20	21	192.168.10.210	20	21

If you have a Web server on your network…

If you enable WAN Management (allow external access from the WAN port, see the *Administration Configuration* section) and want to designate another Web server on your local network, perform either of the procedures below to avoid port conflicts:

Option 1: In the Administration page, with **WAN Management** enabled, enter a port number other than 80 (for example, 1234) and reserve the number 80 for your Web server.

If any external host wants to access your Web management server through the WAN port, it should use the address below:

http://204.71.200.143 (i.e., the WAN IP address):1234

Option 2: Have **WAN Management** use the standard port number 80 and your Web server (e.g., 192.168.10.4) use another port number (e.g., 8080). In this case, you need to shift the incoming HTTP request (destined for local web server) to port 8080 of your Web server, the forwarding entry may look like this:

Start	End	IP Address	Start	End
8080	8080	192.168.10.4	8080	8080

With the settings above, an external host trying to access your local Web server should use an address like this:

http://204.71.200.143 (i.e., the WAN IP address):8080

If you do not enter the suffix :**8080**, the external host's packets will contain the standard port number 80 and the router will not forward the packets since no forwarding entry matches. As a result, if a WAN computer tries to access the LAN's WEB server, it will be routed to the WRC-1000 Web configuration page instead.

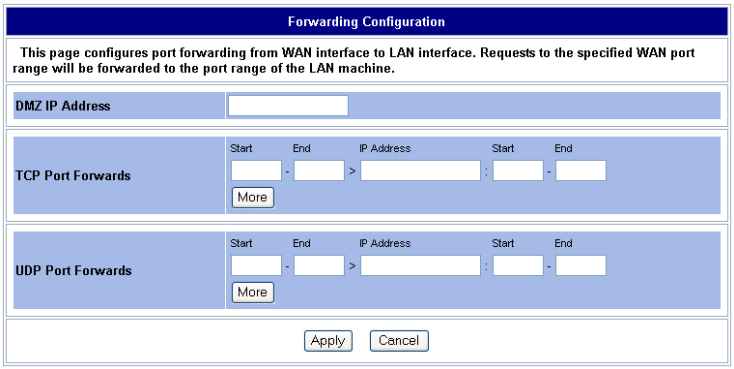


Figure 4-22 Forwarding Configuration

Routing

If your Wireless Routing Center is connected to more than one router or your network is composed of multiple subnets, you may need to set up a static route to determines the data transmitting route. The page displays the routing table of the Wireless Routing Center and allows you to set up a maximum of 8 static routing rules. To add a new static IP route, enter these fields:

Network Address: The destination IP address of the network where data packets are to be sent.

Subnet Mask: The subnet mask of the destination IP address.

Gateway: The IP address of the gateway where data packets are to be sent.

Cost (Hop Count): The number of hops (number of relay routers to go through).

Interface: The interface through which data is forwarded to the next hop.

For example, you want to route the packet destined to the sub-network 192.168.100.0/255.255.255.0 to the next hop 192.168.10.10 and there are 3 routers, the route is as below:

Network Address	Subnet Mask	Gateway	Cost	Interface
192.168.100.0	255.255.255.0	192.168.10.10	3	LAN

After clicking **Apply** to commit your changes, the new route should be added to your routing table. Or you can click the **Update** button on the top to update the routing table.

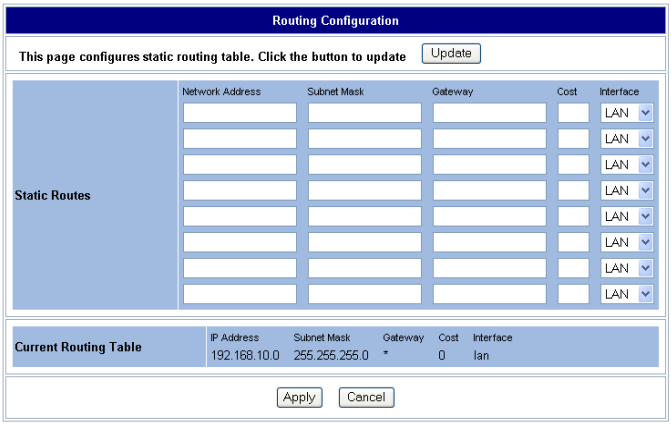


Figure 4-23 Routing Configuration

Administration Configuration

▶ System Clock

Network administrators may want to synchronize date and time among network devices. This can be done by synchronizing the local clock to an available NTP server or manually specifying the date and time in the Wireless Routing Center for your network.

Option 1: Using an existing NTP server

1. In the **Set by** field, enable the **Network Time Protocol** option.
2. In the **NTP Server** field, enter the IP address of the NTP server.
3. In the **Update Interval** field, select **1, 2** or **7** days.
4. In the **Time Zone** field, select a time zone according your geographic location.

Option 2: Manual setting

1. In the **Set by** field, enable the **Manual Setup** option.
2. Type the date and time in their respective fields.

> ***NOTE:*** *Normally, the Administration Configuration Page displays the set values. It is a good idea to check these values periodically to make sure they have not been changed. To verify the current time, refer to the Overview Page.*

▶ Management Setup

Username and **Password:** For administration security, specify the **Username** and **Password** and re-enter the password for confirmation. This setting limits web-based manager access to users with the correct credentials. By default, the user name is **admin** and the password is **password**.

> ***NOTE:*** *These are to authorize access to the Web Configuration Page of the Wireless Routing Center. They are different from the user name and password used to access an Internet Service Provider.*

WAN Management: Available only in NAT Routing Mode. If available, this item is disabled by default. That is, any external access from the WAN port will be rejected. If this option is enabled, a **WAN Port** field is displayed with the default value of 80. If required, you may enter another port number used for external WAN access.

If WAN Management is enabled using a port other than 80, the router's HTTP service (Web Configuration Utility) will be accessible via the router's WAN port IP address followed by a colon and the non-80 port:

http://<WAN IP address>:<non-80 port>

For example, if 1234 is entered, the router will be accessible at http:// 203.1.2.3:1234 where 203.1.2.3 indicates the WAN port's IP address.

If WAN Management is enabled using standard port 80, no suffix is required.

If WAN Management is enabled using port 80, your publicly accessible Web server (if any) on the LAN side should use a non-80 HTTP port. You will need to use the Forwarding feature to shift external HTTP requests to the non-80 port number used by the Web server on the LAN side.

WAN Port Ping Reply: Available only in NAT Routing Mode. If available, this setting determines if an external host will get a reply when trying to ping the IP address of your WAN port. It is disabled by default.

WRC Finder Function Via WAN: Available only in NAT Routing Mode. If enabled, the current settings for Wireless Routing Centers will be displayed when a WAN computer launches this function.

UPnP: Available only in NAT Routing Mode. It allows Windows XP to automatically configure the Router for various Internet applications, such as Windows Messenger®. If available, it is enabled by default.

NetBIOS Communication: Available only in NAT Routing Mode. Port numbers 137~139 and 445 that are used by NetBIOS will be open. It is disabled by default.

Report Log to TFTP Server: Available only in NAT Routing Mode. If available, it specifies whether to report the firewall event log to your TFTP server. If enabled, a **LAN TFTP Server** field is present for you to specify the IP address of the TFTP server. All the filter logs are sent to the TFTP server although only 32 entries are displayed in the **Activity Log** window. (see **Status > Log**).

> ***NOTE:*** *This function is supported only if the IP address of the TFTP server and that of the Wireless Routing Center are in the same subnet.*

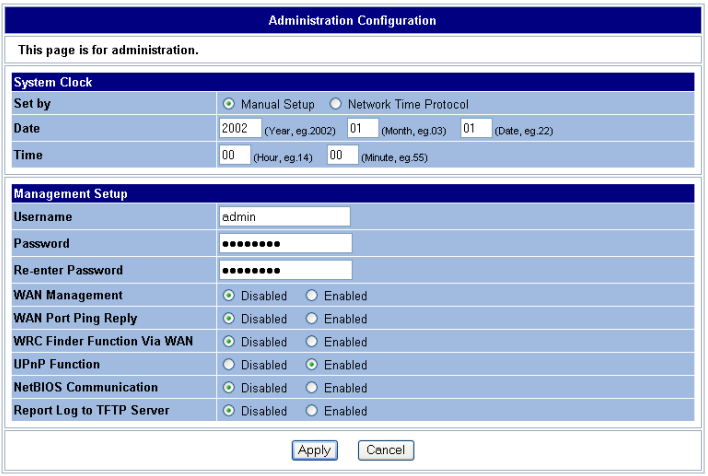


Figure 4-24 Administration Configuration

System Configuration

▶ Firmware Upgrade

This option allows you to upgrade the Wireless Routing Center with new firmware. After upgrading, your customized configurations will still be effective. Upgrading does not revert to the default settings. To upgrade, download the firmware file to your host computer and follow the steps below:

1. In the **Locate New Firmware** field, click **Browse...** to locate the firmware file.
2. Click **Upgrade**. A message will be displayed advising you to wait a few minutes. You will return to the Administration page when the process is complete.

NOTE: Do not interrupt the upgrade process. You could damage your Wireless Routing Center.

After the upgrade is complete, you can see the new firmware version in the **Current Firmware version** field.

▶ User Configurations

Save Current Configurations: Allows you to save your customized settings to the Wireless Routing Center. Once your router is properly configured, you may wish to save current settings. The saved settings can be retrieved easily if required, even after you reload factory defaults.

Retrieve User Configurations: If you have loaded factory defaults (either via the Load Default button on the back panel or via the Restore button in this group), you can restore your last customized settings by clicking the **Retrieve** button.

Restore Factory Defaults: To restore factory defaults, click the **Restore** button and then wait for a few minutes as the utility prompts. You will return to the System configuration page when the process is complete. This feature lets you remotely reset the Wireless Routing Center. Otherwise, the function is the same as resetting via the Load Default button (see the *Back* section in Chapter 2, *The Grant Tour*).

▶ System

Reboot: This option allows to you remotely reboot the Wireless Routing Center.

NOTE: Do not reboot the Wireless Routing Center during data transmission. Rebooting could interrupt data communication.

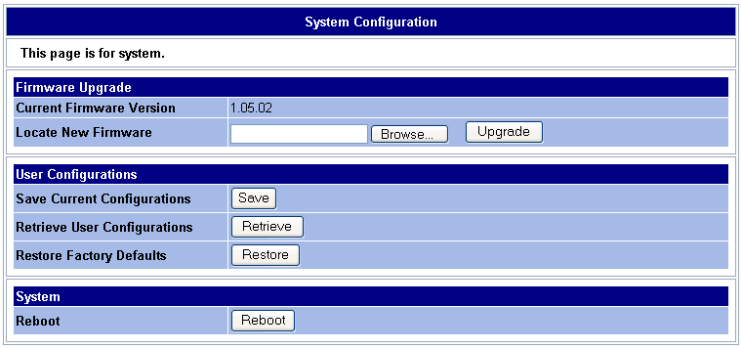


Figure 4-25 System Configuration

Troubleshooting

This chapter provides information on restoring your Wireless Routing Center to proper working order if there appears to be a problem. Refer also to your computer user's manual.

Power

The **Power** indicator does not light when the power switch is pressed.

Cause No power is supplied to the Wireless Routing Center.

Remedy Check the connection of the power cord and AC adapter.

Ethernet

The corresponding Ethernet indicator does not glow when an Ethernet cable is connected.

Cause The cable is not properly connected.

Remedy Refer to the *Setting up the Ethernet/Wireless LAN client* section in Chapter 3, *Setup*, and reconnect the cable.

Cause The cable is inappropriate.

Remedy Refer to the *Setting up the Ethernet/Wireless LAN client* section in Chapter 3, *Setup*, and make sure you are using the proper cable.

Configuration window

The Configuration window does not open, even if the IP address of the Wireless Routing Center is entered in the address box of the browser.

Cause 1 The local IP address of the Wireless Routing Center may be wrong.

Remedy The default local IP address is 192.168.10.1. If it has not been changed, specify this address.

If the local IP address has been changed in **LAN CONFIGURATION**, or if a local IP address different from the default address has been set in the Wireless Routing Center because a DHCP server other than the Wireless Routing Center is in the LAN, enter the set local IP address in the address box of the browser.

If you have forgotten the local IP address, reset to the defaults. Refer to the Appendix A, *Default values*. Note that not only the IP address, but all settings will be reset.

Cause 2 The local IP address set in the personal computer may differ from that of the Wireless Routing Center.

Remedy Confirm that the local IP address of the computer is in the same subnet as the local IP address of the Wireless Routing Center.

To confirm the local IP address of the computer, follow the steps below.

Windows XP/2000

1. Click **Start** and **Run...**.
2. Enter **cmd** to open the Command Prompt window.
3. Enter **ipconfig** and press **Enter**.
4. Check the values for the IP address and subnet mask.

   IP address : 192.168.10.100 - 192.168.10.150

   Subnet Mask : 255.255.255.0

   Default Gateway : 192.168.10.1

Windows 98/Me

1. Click **Start** and **Run...**, then enter **winipcfg** in the input box.
2. In the IP Configuration window, check the network adapter that you want to use.

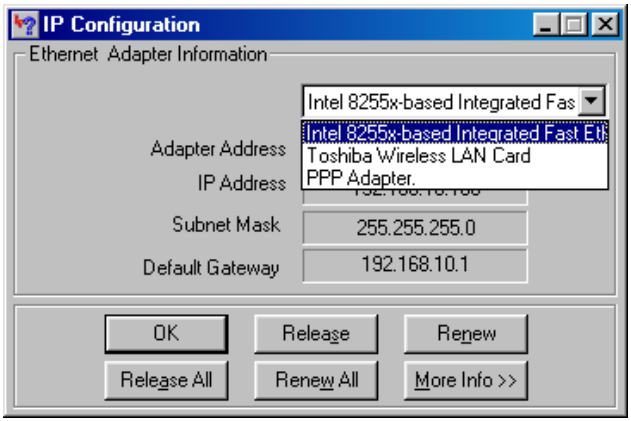


Figure 5-1 Checking Ethernet adapter information

3. Check the values for the IP address and subnet mask in the winipcfg dialog box. In an ordinary small-scale LAN environment, the subnet mask is set to 255.255.255.0.

NOTE: *In the case where the Wireless Routing Center's setting is default, the IP address is 192.168.10.1, Subnet Mask is 255.255.255.0.*

If the TCP/IP protocol has not been installed, or if the correct IP address has not been set, read the manuals for your computer and LAN card and set them accordingly.

Cause 3 The Configuration window might not be displayed if Proxy Server has been set.

Remedy Set not to use Proxy Server. You can enable it later.

The user name and password are not accepted despite repeated entries.

Cause The wrong user name and password have been entered.

Remedy If the **User name** and **Password** was changed in Administrator Account, enter those values. If you have forgotten them, reset to the defaults. Refer to the *Load Default* item in Chapter 2, *The Grand Tour*.

Wireless LAN

There is no communication between a Wireless LAN station and other computers.

Cause 1 The functions of Wireless LAN stations have not been correctly installed.

Remedy Read the manual for your Wireless LAN PC card, and check that the driver has been installed and is operating correctly.

If you are using a TOSHIBA Wireless LAN PC card in a computer running Windows 2000, follow the steps below.

1. Click **Start**, point to **Control Panel** and click **System** to open the dialog for **System Properties**.
2. Click the **Hardware** tab, then double-click **Device Manager**, to open the **Device Manager** window.
3. From the **Network Adapters** item, double-click **TOSHIBA Wireless LAN Card**, to open the **TOSHIBA Wireless LAN Card Properties** dialog box.
4. If the message **This device is working properly** is shown in the item **Device Status**, it indicates that the driver has been installed and is operating.

Cause 2 The settings of Wireless LAN stations are different from those of the Wireless Routing Center.

Remedy Make sure the following settings are the same on the Wireless LAN stations and the Wireless Routing Center.

- SSID (Network Name)
- Basic rate not higher than the communication rate of the Wireless LAN PC cards in the Wireless LAN stations
- WEP mode disable/64 bits/128 bits
- WEP key settings correspond between devices when Encryption is enabled
- Access Control enable/disable
- MAC Address of Wireless LAN PC card correctly registered if Access Control is enabled

Cause 3 TCP/IP has not been set, or has been improperly set at one or more of the computers.

Remedy Confirm that the IP address has been correctly set.

Windows XP

1. Click **Start**, point to **All Programs**, **Accessories** and click **Command Prompt** to open the Command Prompt window.
2. Enter **ipconfig** and press **Enter**.
3. Check the values for the IP address and subnet mask.

   IP address : 192.168.10.100 – 192.168.10.150

   Subnet Mask : 255.255.255.0

   Default Gateway : 192.168.10.1

   If the TCP/IP protocol has not been installed, or if the correct IP address has not been set, read the manuals for your computer and LAN card and set them accordingly.

   If you want to configure the IP address, refer to the *Setting up the Ethernet/Wireless LAN client* section in Chapter 3, *Setup*, for more information.

Windows 2000

1. Click **Start**, point to **Programs**, **Accessories** and click **Command Prompt** to open the Command Prompt window.
2. Enter **ipconfig** and press **Enter**.
3. Check the values for the IP address and subnet mask.

   IP address : 192.168.10.100 – 192.168.10.150

   Subnet Mask : 255.255.255.0

   Default Gateway : 192.168.10.1

   If the TCP/IP protocol has not been installed, or if the correct IP address has not been set, read the manuals for your computer and LAN card and set them accordingly.

   If you want to configure the IP address, refer to the *Setting up the Ethernet/Wireless LAN client* section in Chapter 3, *Setup*, for more information.

Windows 98/Me

1. Click **Start** and **Run...**, then enter **winipcfg** in the input box.
2. Check the values for the IP address and subnet mask in the winipcfg dialog box. In an ordinary small-scale LAN environment, the subnet mask is set to 255.255.255.0.

   In this case, confirm that the first three sets of digits of the IP address of the Wireless LAN station are the same as those of the IP address of the Wireless Routing Center. It corresponds to 192.168.10.x if the Wireless Routing Center's default of 192.168.10.1 is used.

   If you want to configure the IP address, refer to the *Setting up the Ethernet/Wireless LAN client* section in Chapter 3, *Setup*, for more information.

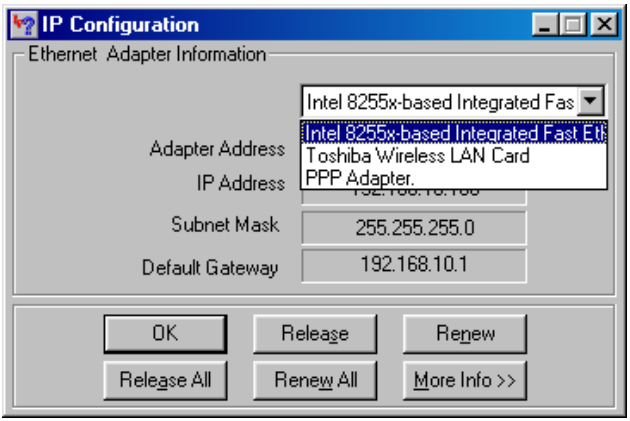


Figure 5-2 Checking the TCP/IP setting

Cause 4 There are incorrect network settings on the computers.

Remedy Following the steps below to make sure the computers can communicate with each other.

Check the domain name and network sharing settings.

1. To open the command prompt, click **Start**, point to **Programs** and **Accessories**. If you are using Window Me, click **MS-DOS Prompt**. If you are using Window 2000, click **Command Prompt**.

   If you are using Windows XP, click **Start**, point to **All Programs**, **Accessories** and click **Command Prompt** to open the Command Prompt.

2. Enter a ping command and the IP address.

   Example: **C:\ping 192.168.10.100**

   Press **Enter**.

   To confirm the IP address of the opposite computer, refer to Cause 4 above.

3. The following message, for example, indicates proper communication. Check the network settings of the computers.

```
C:\ping 192.168.10.100
Pinging 192.168.10.100 with 32 bytes of data
Reply from 192.168.10.100: bytes=32 time<10ms TTL=128
Reply from 192.168.10.100: bytes=32 time<10ms TTL=128
Reply from 192.168.10.100: bytes=32 time<10ms TTL=128
Reply from 192.168.10.100: bytes=32 time<10ms TTL=128
```

4. The following message, for example, indicates improper communication. Check other items of Wireless LAN troubleshooting.

```
C:\ping 192.168.10.100
Pinging 192.168.10.100 with 32 bytes of data
Request timed out.
Request timed out.
Request timed out.
Request timed out.
```

5. If you want to configure IP address, refer to the *Setting up the Ethernet/Wireless LAN client* section in Chapter 3, *Setup*, for more information.

Application problems

Some network applications do not work.

Cause The Wireless Routing Center uses NAT to convert the IP addresses and port numbers in the headers of packets in communication between LAN and WAN. Therefore, applications that use IP addresses and port numbers kept in the data part of packets may not work as expected due to differences between the packet header and packet data in terms of IP addresses and port numbers.

Applications using a protocol other than TCP/UDP might not operate properly due to non conversion of port numbers by NAT because there is no port number in the header.

Remedy These applications do not operate normally with the Wireless Routing Center. If you know their port numbers, however, they might be usable by registering the port numbers using Port Forwarding. For details, see the *Forwarding* section in Chapter 4.

Forgotten password

- Password to go to the Wireless Routing Center's Configuration window:

  Set the Wireless Routing Center to the defaults. Refer to the Appendix A, *Default values*.

Default setting

	User Name	Password
Administrator Account	admin	password

- Password to access Internet Service Provider

  Call the customer support office of your Internet Service Provider.

Question

Can the Wireless Routing Center be used with Linux?

TOSHIBA confirmed the operation of the Wireless Routing Center with Linux using TCP/IP, but offers no guarantee of operation. It is outside the scope of support.

Appendix A

Default values

The table below lists all the Wireless Routing Center's default values. Values that are not listed are blank. To reset the Wireless Routing Center, refer to the *Load Default* item in Chapter 2, *The Grand Tour*.

WAN

WAN/LAN Relation	NAT Routing mode
Protocol	DHCP Client

LAN

IP Address	192.168.10.1
Subnet Mask	255.255.255.0
DHCP Server Service	enable
DHCP Lease Time	72 hours
IP Pool Range	192.168.10.100~192.168.10.150

Wireless LAN

Access Point Name	WRC-1000_AP
Network Name	WRC_Network
Channel ID	10
Do not broadcast SSID	disable
Beacon Interval	100
RTS Threshold	2346
Fragmentation Threshold	2346
Basic Rate	1 and 2 Mbps
Supported Rate	1, 2, 5.5 and 11 Mbps

Wireless LAN Security

802.1x	Not Used
WEP Mode	disable
Authentication Mode	Open
MAC Address Access Control	disable

Filters

Filter Type	Listed Block
MAC Filters	disable
IP Filters	disable
TCP Port Filters	disable
UDP Port Filters	disable

Administration

System Clock set by	Manual Setup
Username	admin
Password	password
WAN Management	disable
WAN Port Ping Reply	disable
WRC Finder Function Via WAN	disable
UPnP Function	enable
NetBIOS Communication	disable
Report Log to TFTP Server	disable

802.1x

Overview

The 802.1x function restricts the connection of unauthorized stations by authenticating each station.

The 802.1x function has the following advantages in security and administration.

Security The function makes authentication during station connection and permits only the station that has passed the authentication to communicate. This function makes it difficult for an unauthorized station to get in the network.

Administration Because the function dynamically distributes the WEP key, the Encryption (WEP) key does not need to be set at each station.

NOTES: *1. Although several authentication methods are available, the WEP key cannot be distributed in some of those methods.*

2. If 802.1x is enabled, the following conditions apply:

a. 802.1x disabled Wireless LAN clients CANNOT communicate with LAN clients connected with the Wireless Routing Center's ethernet ports.

b. 802.1x enabled Wireless LAN clients CAN communicate with LAN clients connected with the Wireless Routing Center's ethernet ports.

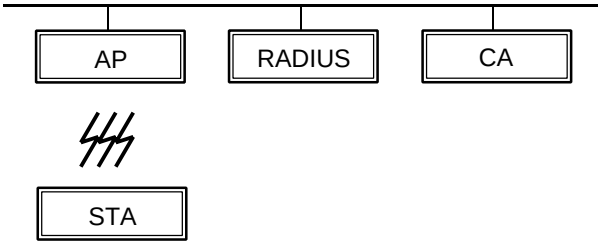
c. Wireless LAN clients CAN communicate with each other regardless of which client's 802.1x functions are enabled or disabled.

802.1x Function

This section explains the 802.1x function more specifically.

Required Environment

The following environment is required to use the 802.1x function.



AP	Access point (this product).
STA	Wireless LAN station The 802.1x function needs to be supported even on the station side.
RADIUS	Abbreviation of Remote Authentication Dial In User Service. This server authenticates STAs.
CA	Abbreviation of Certificate Authority. This sever issues a digital certificate. This server is required to use an authentication type that is called EAP-TLS (Smart Card or other certificate).

NOTE: *The above terms (abbreviations) are used in the subsequent explanations.*

Authentication and Distribution of WEP Key

This section explains authentication (re-authentication) and the distribution of the WEP key.

Authentication

Authentication starts when a radio LAN station connects to the access point.

When the station connects, the access point issues a request to start authentication for that station. Although the station that has received the request starts the authentication procedure, the access point transfers all messages related to the authentication to the RADIUS server. That is, the authentication itself is performed between the station and RADIUS server.

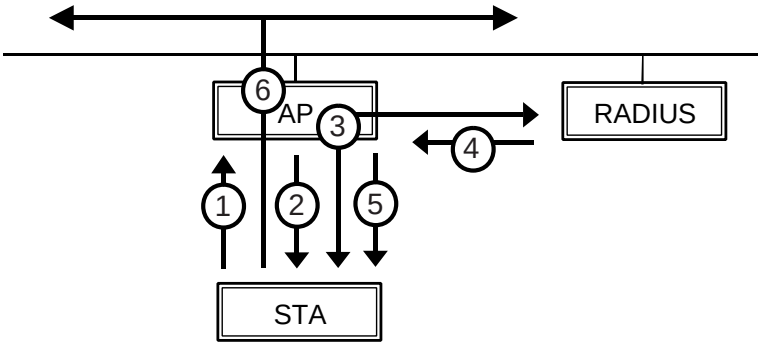
While the authentication procedure is performed, the station cannot join the network.

When the station passes the authentication, the RADIUS server reports to the access point.

The access point will then allow the station to join the network.

The following shows the authentication procedure (successful example).

Authentication procedure (successful example)



1. The station connects to the access point.
2. A request to start authentication is sent from the access point to the station.
3. The authentication procedure is performed between the station and RADIUS server.
4. The RADIUS server reports to the access point that the station has passed the authentication.
5. The access point reports to the station that the station has passed the authentication.

The access point permits the station to communicate.

At this point, the WEP key can be distributed. (Whether the WEP key can be distributed depends on the authentication type.)

6. The station can joint the network.

Authentication type

Several types of authentication are prepared. The radio LAN station and RADIUS server need to predetermine which type of authentication to use mutually. If different types of authentication are set, the authentication procedure cannot be performed and the authentication of the station fails. Whether the WEP key can be distributed depends on the authentication type.

The following lists the typical types of authentication.

Name	Description
MD5-Challenge	Authentication method using the user name and password In this type of authentication, the WEP key cannot be distributed.
EAP-TLS	Authentication method using a digital certificate. It may be represented by "Smart Card or other certificate." To use this type of authentication, the certificate needs to be obtained from the CA and stored in each station. In this type of authentication, the WEP key can be distributed.

Distribution of WEP key

When authentication ends successfully, the access point distributes the WEP key to the station. (Whether the WEP key can be distributed depends on the authentication type.)

The WEP key is created at random by the access point.

Configuration Example

This section explains how to establish the 802.1x environment, giving specific examples.

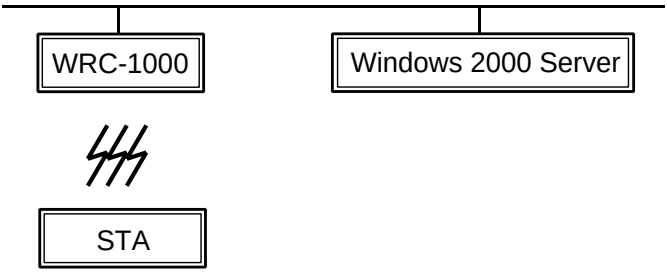
Configuration Example

The environment is established, based on the following scenario.

- All stations support the 802.1x function. (Windows XP is used.)
- The WEP key to be distributed is 128 bits.
- The CA uses “Certificate Services” of Windows 2000 Server.
- The RADIUS uses “Internet Authentication Service” of Windows 2000 Server.

Device configuration

The following is the device block diagram.



Windows 2000 Server	Software	Windows 2000 Server is used as the OS. The RADIUS uses “Internet Authentication Service.” The CA uses “Certificate Services.”
WRC-1000		
STA	Software	Windows XP is used as the OS.
	Hardware	A radio LAN card with WEP 128 bits is used.

CA (Certificate Authority)

Install Certificate Service in Windows 2000 Server.

For details on Certificate Service, refer to the online Help of Windows 2000.

RADIUS server

Install Internet Authentication Service in Windows 2000 Server.

For details on Internet Authentication Service, refer to the online Help of Windows 2000.

Step 1 Client setting

Make client settings in the following procedure.

1. Start **Internet authentication service** in **`Administrative Tools`**.
2. Select **Client** in the **`Tree`** window and click the right mouse button.
3. Select **New Client** from the menu.
4. Set **Friendly name**. In this example, **`WRC-1000AP`** is set.

   Leave the other items in the default setting.

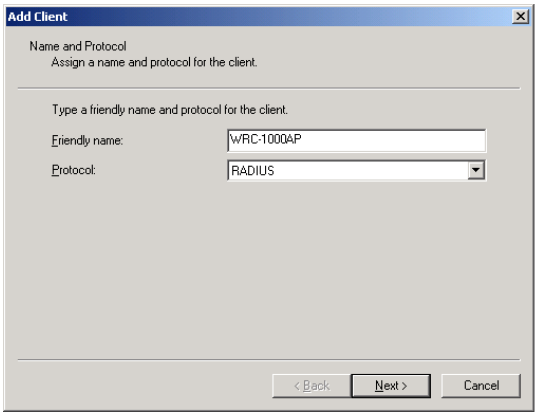


Figure B-1 Add Client window

Click **Next**.

5. Set **Client address**. Enter the IP address of the access point and RADIUS server. In this example, **`192.168.10.1`** is set.

   Set **Shared secret**. Enter the password for communication between the access point and the RADIUS server. In this example, **`my shared secret`** is set.

   Leave the other items in the default setting.

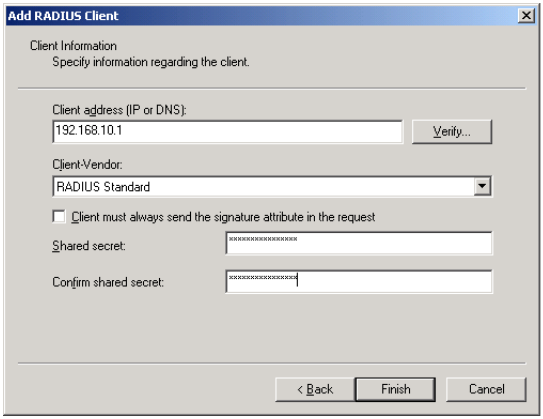


Figure B-2 Add RADIUS Client window

Click **Finish**.

Step 2. Setting Remote Access Policies

1. Select **Remote Access Policies** in the **`Tree`** window and click the right mouse button.
2. Select **New Remote Access Policy** from the menu.

3. Set **Policy friendly name**. In this example, **WRC-1000AP** is set.

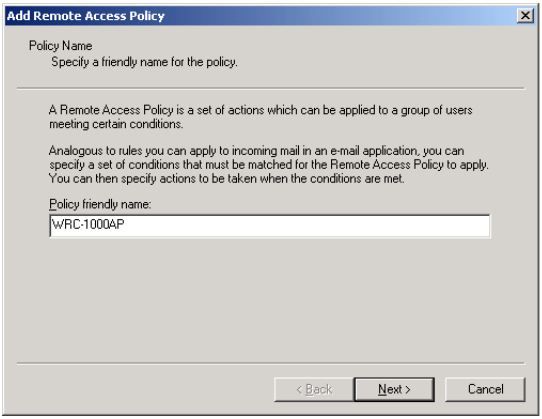

Add Remote Access Policy
Policy Name
Specify a friendly name for the policy.
A Remote Access Policy is a set of actions which can be applied to a group of users meeting certain conditions.
Analogous to rules you can apply to incoming mail in an e-mail application, you can specify a set of conditions that must be matched for the Remote Access Policy to apply. You can then specify actions to be taken when the conditions are met.
Policy friendly name:
WRC-1000AP
< Back
Next >
Cancel

Figure B-3 Add Remote Access Policy window

Click **Next**.

4. Add a **Conditions** by pressing the **Add** button. This example defines that this policy should be used when **Client-Friendly-Name** is **WRC-1000AP**. Various conditions are available. For details, refer to Windows 2000 online Help.

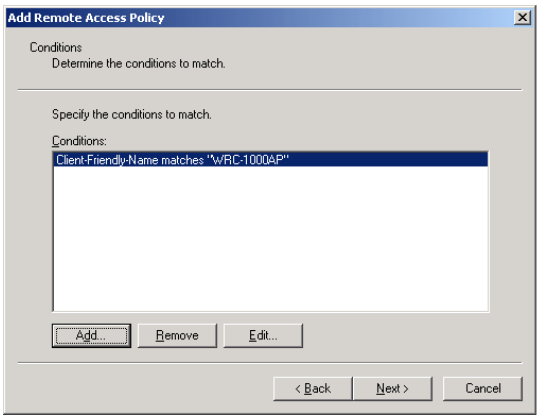


Figure B-4 Add a Conditions window

Click **Next**.

5. Select **Grant remote access permission**.

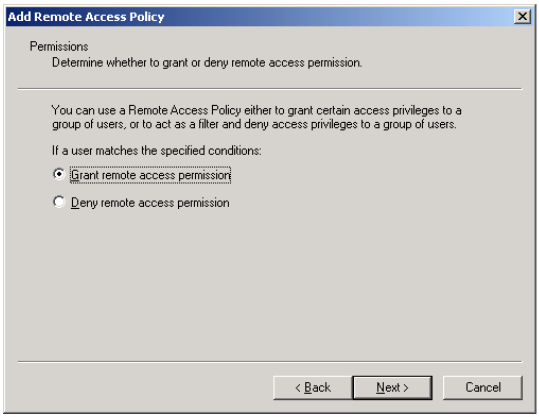

Add Remote Access Policy
Permissions
Determine whether to grant or deny remote access permission.
You can use a Remote Access Policy either to grant certain access privileges to a group of users, or to act as a filter and deny access privileges to a group of users.
If a user matches the specified conditions:
Grant remote access permission
Deny remote access permission
< Back
Next >
Cancel

Figure B-5 Select Grant remote access permission

Click **Next**.

6. Click the **Edit Profile** button and select the **Authentication** tab.
   Place a check mark in the **Extensible Authentication Protocol** check box.
   Select **Smart Card or other Certificate** for the EAP type.

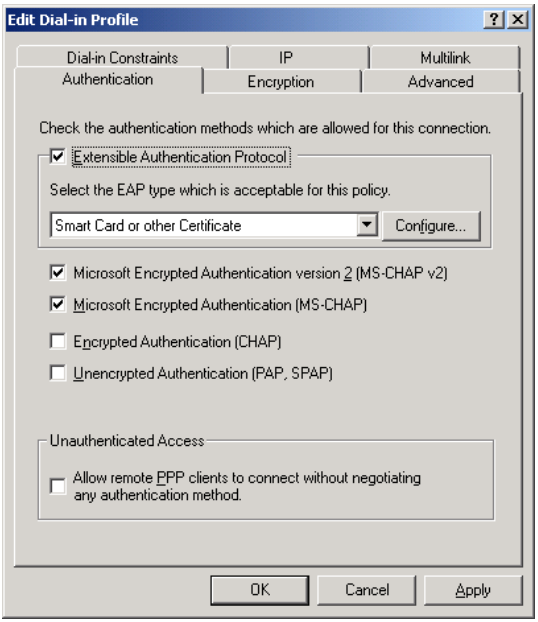


Figure B-6 Edit Dial-in Profile window

Click **OK**.

Click **Finish**.

Access point

The following is the setting procedure for the access point.

Step 1 Setting the 802.1x function at the access point

Make settings for the 802.1x function.

The following procedure is to enable the 802.1x function. The other settings of the **Wireless LAN** page is omitted.

1. Open the default page on the Web.

2. Select the **Wireless LAN Security** page.
3. 802.1x group

   Select **Used** in the **802.1x** field.

   Select the **Enable** radio button in the **WEP Key Distribution** field.

   Select the **128bits** radio button in the **Key Length** field.
4. RADIUS group

   Select the **1 Enable** radio button in the **RADIUS Servers** field.

   Set a value in the **IP Address** field. Enter the IP address of the RADIUS server. In this example, set **192.168.10.10**.

   Set a value in the **Port** field. In this example, set **1812**.

   Set a value in the **Shared Secret** field. Shared secret is a password for communication between the access point and the RADIUS server. In this example, set **my shared secret**. The characters you enter in this field will be displayed as ●.

   Set a value in the **Time-out** field. In this example, set **5**.

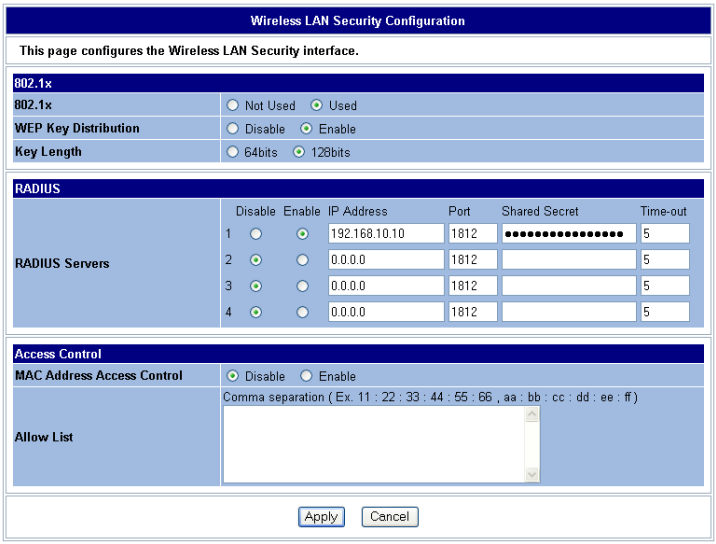


Figure B-7 Setting the 802.1x and RADIUS groups window

Wireless LAN station

The following provides the setting procedure for the Wireless LAN station.

Step 1 Certificate issuance and installation

First, have the certificate organization issue a certificate and store it in the local computer.

1 Temporarily, have the station join the wired LAN network.

2 Start the Internet Explorer and connect to the following URL.

http://(the CA's IP address)/certsrv

Then, install the certificate according to instructions on the screen.

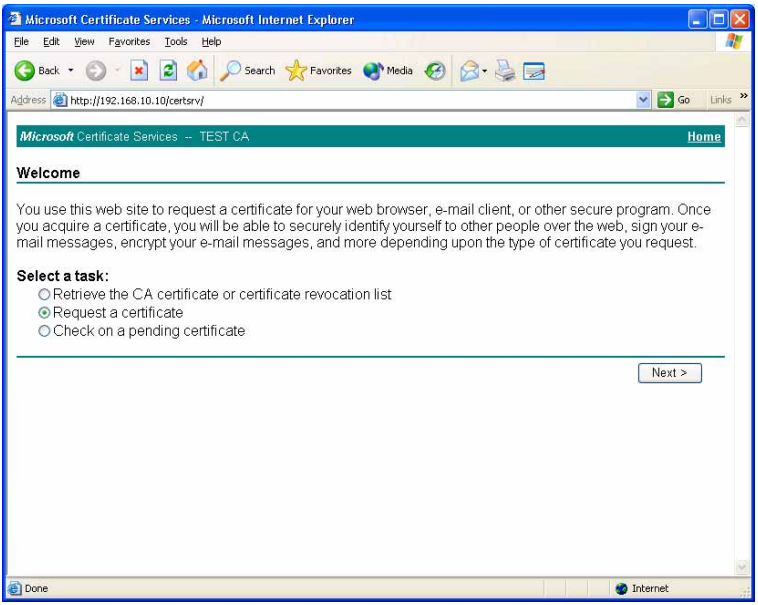

Microsoft Certificate Services - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://192.168.10.10/certsrv/
Go Links
Microsoft Certificate Services -- TEST CA
Home
Welcome
You use this web site to request a certificate for your web browser, e-mail client, or other secure program. Once you acquire a certificate, you will be able to securely identify yourself to other people over the web, sign your e-mail messages, encrypt your e-mail messages, and more depending upon the type of certificate you request.
Select a task:
Retrieve the CA certificate or certificate revocation list
Request a certificate
Check on a pending certificate
Next >
Done
Internet

Figure B-8 Certificate Installation

NOTES: *1. To issue a certificate from the certificate authority and install it, [Certificate Service Web Enrollment Support] needs to have been installed in the certificate authority.*

2. *The above example issues and installs a certificate through the network. You can also download the certificate into a file and install it from media such as a floppy disk. For more information, refer to the online Help of the certificate authority.*

Step 2. Setting the 802.1x function in the Wireless LAN station

Next, set the 802.1x function.

The following procedure is to enable the 802.1x function. The other settings for the radio LAN network are omitted.

For details on each item, refer to the online Help of Windows XP.

1. Open **Wireless Network Connection Properties**.

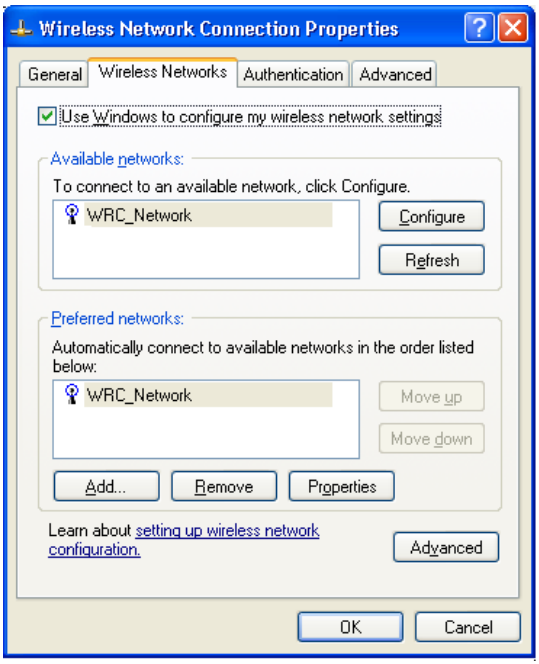


Figure B-9 Wireless Network Connection Properties window

2. Select the **Authentication** tab.

   Place a check mark in the **Enable network access control using IEEE 802.1x** check box.

   Select **Smart Card or other Certificate** in the **EAP type** field.

   Click **Properties**.

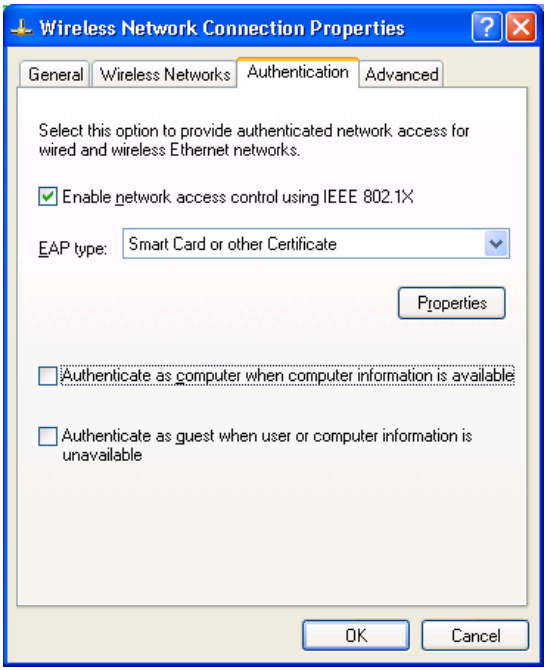

Wireless Network Connection Properties
General
Wireless Networks
Authentication
Advanced
Select this option to provide authenticated network access for wired and wireless Ethernet networks.
Enable network access control using IEEE 802.1X
EAP type:
Smart Card or other Certificate
Properties
Authenticate as computer when computer information is available
Authenticate as guest when user or computer information is unavailable
OK
Cancel

Figure B-10 Authentication tab

3. Select the **Use a certificate on this computer** radio button.

   Place a check mark in the **`Validate server certificate`** check box.

   Select a reliable certificate authority from the **`Trusted root certificate authority`** combo box.

   In this example, select the certificate authority, which was installed in Windows 2000 Server.

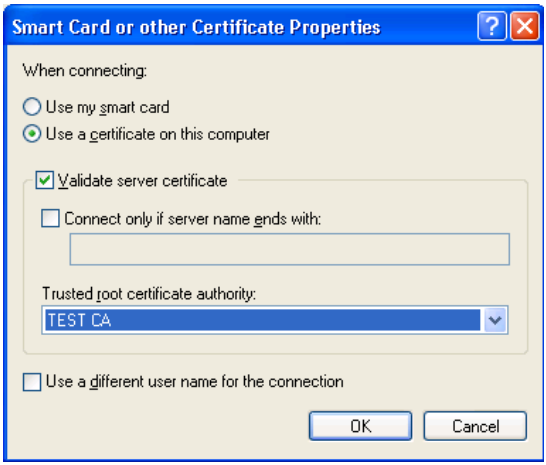

Smart Card or other Certificate Properties
When connecting:
Use my smart card
Use a certificate on this computer
Validate server certificate
Connect only if server name ends with:
Trusted root certificate authority:
TEST CA
Use a different user name for the connection
OK
Cancel

Figure B-11 Properties window

Check items

Check whether authentication ended successfully as follows.

- Check the Windows 2000 Server system log for source name IAS.
- Check the status of the radio LAN adaptor on the Windows XP network control panel.

AC Power Cord and Connectors

The power cord's AC input plug must be compatible with the various international AC power outlets and the cord must meet the standards for the country/region in which it is used. All cords must meet the following specifications:

Length:	Minimum 1.8 meters (5.9 ft.)
Wire size:	Minimum 0.75 mm^2
Current rating:	Minimum 2.5 amperes
Voltage rating:	125 or 250 VAC (depending on country/region's power standards)

Certification agencies

U.S. and Canada: UL listed and CSA certified

No. 18 AWG, Type SVT or SPT-2 two conductor

Europe:

Austria:	OVE	Italy:	IMQ
Belgium:	CEBEC	The Netherlands:	KEMA
France:	UTE	Germany:	VDE
United Kingdom:	BSI		

Australia: AS

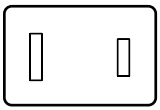
Japan: DENANHO

In Europe, power cords must be VDE type, H05VVH2-F and two conductor.

For the United States and Canada, plug configuration must be a 2-15P (250 V) or 1-15P (125 V) as designated in the U.S. National Electrical code handbook and the Canadian Electrical Code Part II.

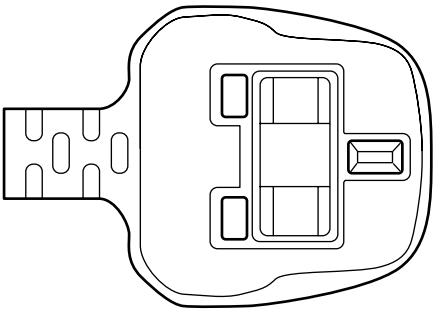
The following illustrations show the plug shapes for the U.S.A. and Canada, the United Kingdom, Australia and Europe.

USA and Canada



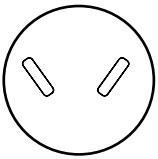
UL approved
CSA approved

United Kingdom



BS approved

Australia



AS approved

Europe

Approved by the appropriate agency

Glossary

The terms in this glossary cover the topics discussed in this manual.

10Base-T/100Base-TX: Two standards for Ethernet data transmission speeds. 10Base-T transmits at 10Mbps and 100Base-TX transmits at 100Mbps.

A

access point name: The access point name is used to identify a device access point in a wireless LAN environment.

ADSL: Asymmetric Digital Subscriber Line is a modem technology that enables high-speed data communications over existing phone lines. A splitter enables simultaneous transmission of voice/fax and digital data.

B

bridge: A bridge connects LANs. They also improve efficiency of transmission within a LAN. A basic bridge has ports connected to two (or more) otherwise separate LANs. Packets received on one port may be retransmitted on another port. A bridge will not start re-transmission until it has received the complete packet. Therefore, stations on either side of a bridge may be transmitting simultaneously without causing collisions.

C

channel: The channel is the radio frequency used to communicate on a wireless LAN. Wireless LANs use the frequency band of 2.4 GHz divided into two or more subchannels. Usable channels are restricted by the regulations in each country. Channels 1 to 11 are usable in the United States, for example.

D

default gateway: A gateway is an interface between networks. The default gateway is the one that is used generally or when a specific gateway is not designated.

DHCP: Dynamic Host Configuration Protocol automatically sets TCP/IP network information, such as an IP address in each computer accessing the Internet.

DNS: Domain Name System is an Internet protocol for mapping host names, domain names and aliases to IP addresses.

DNS relay: When a DNS client sends a request to a DNS server, it does not go directly to a server, instead it is routed through a DNS relay. The DNS server's reply is also routed through the DNS relay, which sends it to the DNS client.

E

encryption: The device allows use of data encryption compliant with the IEEE802.11 standard WEP (Wired Equivalent Privacy) and 128 bit WEP. Data encryption protects your data from external access.

ESSID: See network name.

G

global IP address: A global IP address is used to identify a computer directly connected to the Internet. It is assigned by a public organization such as the Network Information Center.

H

hidden station problem: Hidden stations are terminals (for example, computers with a wireless LAN card installed) that can communicate with a common access point, but are in a position where the signals from one cannot reach the other. If hidden terminals try to contact the access point at the same time, their trans-missions cannot be properly received and retries will result, thereby degrading LAN operation.

I

IEEE 802.1x: A standard for verifying users on a LAN. Transmissions from unverified users are blocked. Only verified users are allowed to transmit on the LAN.

IEEE 802.11b (IEEE 802.11): A wireless LAN standard that enables data transmission at a speed of 11 Mbps and a wave length of 2.4GHz. Devices can be located up to 100 meters from the access point.

infrastructure mode: When the LAN transmissions are made through an access point.

IP address: Internet Protocol Address is a unique 32-bit addresses assigned to each node on networks that use IP.

ISP: Internet Service Provider is a company that provides server computers for connection to the Internet.

L

local IP address: A local Internet Protocol Address is a unique 32-bit addresses assigned to each node on a LAN using the TCP/IP standard.

LAN: A Local Area Network is a computer network limited to the immediate area, usually the same building or floor of a building.

M

MAC address: The Media Access Control address is your computer's unique hardware number that identifies it on a LAN.

MAC address filtering: Ensures that only computers that are registered with the device will be allowed access, either to the Internet or to a wired LAN.

medium reservation: Reserving the access point for a specific terminal and notification to other terminals not to call. It is used to avoid the hidden terminal problem.

N

NAT: Network Address Translation enables multiple users to simultaneously share a single global IP address. When a computer accesses the Internet, the NAT function uses a table to convert global and local IP addresses and ports.

network name: A network name identifies groups communicating with each other over a Wireless LAN.

P

port: The port (port number) is used to determine which application should handle a TCP or UDP packet.

port forwarding: Connects a local IP address and port number to a global address. When a client computer issues a request to the Internet, the request goes through the device, which uses the NAT table to connect the client's local address and port number to a global address. The reply is received by the device which relays it to the client computer.

PPP: PPP is a protocol to authenticate computers communicating with each other in a network, such as a personal computer connected by phone line to a server.

PPPoE: Point-to-Point Protocol over Ethernet.

protocol: A set of rules used for transmitting data.

Proxy server: A proxy server acts as a connection point between a network and the Internet and serves as an agent for computers in the network. Proxy server can refer to either a computer or to a software server.

R

RADIUS: A verification system for client-server dial-up connections. It verifies the user making a dial-up connection to the access server.

Reject unspecified network name: A function that restricts access to the LAN to terminals that have the same network name as that of the access points.

router: A device (or software package) that handles the connection between 2 or more networks. Routers spend all their time looking at the destination addresses of the packets passing through them and deciding which route to send them on.

routing: Determining the path for a packet to travel and managing the transmission of the packet.

routing table: A table containing routing information such as network address, the next relay router and hop count.

S

static routing: A routing system in which routes are set manually.

subnet mask: Determine what subnet an IP address belongs to.

switching hub: A multiport bridge that receives data packets compares the address to an address table and relays the data to the proper port.

T

TCP/IP: Transmission Control Protocol/Internet Protocol are protocols data transmission over the Internet.

TCP: Transmission Control Protocol is a protocol to establish a connection between two computers. It the includes error correction for packet transmission. Compare UDP.

U

UDP: User Datagram Protocol is part of the TCP/IP suite of protocols. UDP is a connectionless protocol for data transmission that does not acknowledge whether packets are received or not. It enables faster performance but, there is no assurance of an accurate transmission.

UPnP: Universal Plug and Play is designed to support zero-configuration. It allows Windows XP to automatically configure the Router for various Internet applications, such as Windows Messenger®.

W

WAN: Wide Area Network covers a larger area than a LAN. See also LAN.

WEP key: See encryption.

wireless LAN access point: A terminal on a wireless LAN or an interface between a wireless LAN and a wired LAN.

wireless LAN PC: A personal computer connected to a LAN through radio communication.

wired LAN PC: A personal connected to an Ethernet LAN by cable.

Index

A

AC adapter 2-6, 3-4
AC Power Cord and Connectors C-1
Administration configuration 4-30
  management setup 4-30
  system clock 4-30

B

Bridge mode 4-16
Browser 4-2

C

Configuration 4-1
  features list 1-3
  overview page 4-5, 4-6
  retrieve 4-33
  save 4-33
  WEB configuration page 4-2

D

DC IN jack 2-2
Defaults
  load default switch 2-2
  restore 4-33
  values A-1
DHCP 1-2

E

Encryption 4-21
Ethernet features 1-1

F

Filters
  log 4-26
  rules 4-23
  types 4-24
Finder, *See* WRC finder
Firmware upgrade 4-32
Forwarding 4-26

I

Indicators
  icons 2-3
  LED table 2-4
  location 2-1
Initialize switch, *See* Defaults, load default switch

L

LAN
  client set-up
    Ethernet 3-7
    wireless 3-11
  configuration 3-7
  connections 3-5
  DHCP settings 3-7
  IP settings 3-7
  ports 2-2
Log 4-7

M

Mounting
  horizontal 3-3
  vertical 3-2
  wall 3-4

N

NAT routing mode 4-9
  LAN configuration 4-13
  WAN configuration 4-9

P

Password 4-5, 4-11
Ping 3-12
Ports 2-2
Power switch 2-2

R

Reboot 4-33
Router features 1-2
Routing configuration 4-29

S

Security 1-3
  802.1x B-1
    Configuration Example B-5
    Function B-2
    Overview B-1
    WEP Key B-2
  Features list 1-3
  Wireless LAN 4-19
    802.1x 4-20
    access control 4-22
    RADIUS Server 4-22
    WEP 4-20
Stand 2-5
Startup 3-7
System configuration 4-32
  firmware upgrade 4-32
  user configurations 4-33
System requirements 1-1

T

Troubleshooting 5-1
  application problems 5-7
  configuration window 5-1
  Ethernet 5-1
  forgotten password 5-8
  Linux 5-8
  power 5-1
  Wireless LAN 5-3

U

User name 4-11

W

WAN
  connection 3-5
  port 2-2
WRC Finder 4-2
Wireless LAN, *See also* Security
  configuration 4-18
    advanced 4-19
    basic 4-18
  features list 1-3